EXHIBIT M

~~SECRET//COMINT//~~ [redacted]

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

Issue Date: 11 March 2004
Revised: 27 December 2007,
29 May 2009

(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 5240.01 (Reference a), which implements 50 U.S.C. 1801 et seq (the Foreign Intelligence Surveillance Act of 1978, as amended (Reference b)); Executive Order 12333, as amended (Reference c); and Executive Order 12863 (Reference d). It establishes procedures and assigns responsibilities to ensure that the signals intelligence and information assurance missions of 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 policies and instructions, and internal NSA/CSS policy.

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

//s//

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

Endorsed by
Associate Director for Policy

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

DISTRIBUTION:
DJP1
DJP2 (VR)
DJP2 (Archives)

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20291123~~

(U) This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998. The Associate Director for Policy endorsed an administrative update, effective 27 December 2007 to make minor adjustments to the policy. This 29 May 2009 administrative update includes changes due to the FISA Amendments Act of 2008 and in core training requirements.
(U) OPI: Office of General Counsel (OGC), 963-3121s
(U) No section of this document, regardless of classification, shall be released without approval from the Office of Policy and Records, DJP1.

(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), orders issued by the Foreign intelligence Surveillance Court pursuant to reference b, 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, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. NSA/CSS shall intentionally collect only foreign communications. NSA/CSS shall not intentionally collect U.S. person communications without proper legal authorization. The Director, NSA/Chief, CSS (DIRNSA/CHCSS) 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 and the Director of National Intelligence issued pursuant to Section 105(b) of the Act. The DIRNSA/CHCSS or Deputy Director, NSA (D/DIR) must approve applications for a court order, which must be submitted through the DoD General Counsel to the Attorney General. The DIRNSA/CHCSS or D/DIR 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 an order by the Foreign Intelligence Surveillance Act Court. In emergency situations (e.g., U.S. hostages overseas), as described in Procedure 5, Part 2., of Reference e, the DIRNSA/CHCSS, D/DIR or Senior Operations Officer at the National Security Operations Center may authorize electronic surveillance, after consulting with the Office

of General Counsel (OGC). The Attorney General shall be notified promptly of any such surveillance.

3. (U) Information Assurance. National Security Directive (NSD) 42 (Reference g) and Executive Order 12333 (Reference c) designated DIRNSA as the National Manager for National Security Systems (e.g. NSA's Information Assurance (IA) mission) as that term is defined by 44 U.S. C. 3542(b)(2) (Reference h). In that capacity, and pursuant to those authorities as well as other applicable laws and policies, DIRNSA's responsibilities include examining national security systems and evaluating their vulnerability to foreign interception and exploitation. NSA, as an element of the Intelligence Community and pursuant to section 2.6(c) of Executive Order 12333, as amended, may provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any U.S. Government department or agency having a national security system or a non-national security system. The Executive Order directs that provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department. The Federal Information Security Management Act of 2002 (Reference i) and implementing procedures agreed to by NSA/CSS and the National Institute of Standards and Technology also authorizes NSA/CSS to provide IA support for US government non-national security systems.

a. (U) Any IA activities undertaken by NSA/CSS, 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.

b. (U) 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.

c. (U) Pursuant to NSA/CSS Policy 1-2, "(U) Mission and Functions Statements with Service Level Agreements," (Reference l) and IAD's Mission and Functions Statement (Reference m), IAD performs all functions on behalf of the DIRNSA in fulfilling his role as National Manager for National Security Systems. Accordingly, the Information Assurance Director acts for DIRNSA/CHCSS in the issuance of written approval to conduct the information assurance activities assigned to NSA/CSS, including the conduct of activities that may result in the collection of U.S. 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 identify and prevent violations of Executive Order (E.O.) 12333, DoD Directive 5240.1 (References c and a), this Policy, and any laws, orders, directives and regulations; and

b. (U) Forward to the Intelligence Oversight Board (IOB) of the President's Intelligence Advisory Board (PIAB), through the Assistant to the Secretary of Defense for 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 other questionable intelligence activities or significant or highly sensitive matters, as well as provide other reports or information that the IOB or ATSD(IO) requires.

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;

b. ~~(S//REL)~~ Perform general oversight of the SIGINT activities of the [redacted] for compliance with E.O. 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 DIRNSA/CHCSS and D/DIR on the results of the IG's oversight activities; and

f. (U) Report, as required by E.O. 12333, E.O. 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 any NSA organization, all new major requirements and internally generated NSA/CSS activities;

e. (U) Advise appropriate NSA organizations of new legislation and case law which may have an impact on NSA/CSS missions, functions, operations, activities, or practices;

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 FISA, as amended (Reference b);

g. (U) In conjunction with the OIG, report as required by E.O. 12333 and E.O. 12863 (References c and d) to the ATSD(IO) and the PIOB, and provide copies of such reports to DIRNSA/CHCSS and affected NSA/CSS elements;

h. (U) Prepare and process applications for authority to conduct electronic surveillance pursuant to law, Executive Order and policy; and

i. (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 Directors, Associate Directors, the NSA/CSS Chief of Staff, and Extended Enterprise Commanders/Chiefs 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), except *contractor personnel excluded from core training requirements*, 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, except contractor personnel excluded from core training requirements, 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 not excluded from core training requirements 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. Signals Intelligence Directive SP0018 (USSID SP0018) (Reference n), and employees involved in COMSEC monitoring must be familiar with NTISSD 600 (Reference j).

c. (U) Apply the provisions of this Policy to all activities under their cognizance and ensure that all publications (U.S. Signals Intelligence 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/CSS 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 preparing the joint Inspector General/General Counsel/Director, NSA/ CSS quarterly report to the Assistant to the Secretary of Defense (Intelligence Oversight) and the IOB; and

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. These 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 5240.01, "DoD Intelligence Activities," dated August 27, 2007.

b. (U) "Foreign Intelligence Surveillance Act of 1978," as amended, 50 U.S.C. 1801 et seq.

c. (U) Executive Order 12333, "United States Intelligence Activities," as amended.

d. (U) Executive Order 12863, "President's Foreign Intelligence Advisory Board," dated 13 September 1993.

e. (U) DoD Regulation 5240. l-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," dated 7 December 1982.

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. [Intelink]

i. (U) "Federal Information Security Management Act of 2002," Public Law 107–347, date 17 December 2002.

j. (U) National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring," dated 10 April 1990.

k. (U) "Homeland Security Act of 2002, Title II ," Public Law 107-296.

l. (U) NSA/CSS Policy 1-2, "(U) Mission and Functions Statements with Service Level Agreements," dated 12 May 2003.

m. (U) NSA/CSS Mission and Functions Statement for Information Assurance Directorate, dated 23 April 2003.

n. (U) United States Signals Intelligence Directive (USSID) SP0018, "Legal Compliance and Minimization Procedures," dated 27 July 1993.

o. (U//~~FOUO~~) Memorandum from the Assistant to the Secretary of Defense to the Director, National Security Agency, "Exemption from Specified Training Requirements Required by Department of Defense (DoD) Regulation 5240.1-R," dated 3 December 2008.

p. (U) National Security Council Intelligence Directive (NSCID) No. 6, "Signals Intelligence," dated 17 February 1972.

(U) DEFINITIONS

9. (U~~//TOUO)~~ Contractor Personnel Excluded from Core Training Requirements – Refer to the Secret//Not Releasable to Foreign Nationals memorandum from the Assistant to the Secretary of Defense, dated 3 December 2008 (Reference o), for contractor personnel in this category.

10. (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.

11. (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 p), 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.

12. ~~(C//REL)~~ 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 non-governmental 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 SP0018 (Reference n), Section 9.18.

(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. Further, these procedures do not apply to signals intelligence activities directed against the radio communications of air and sea vessels for the purpose of collecting foreign intelligence regarding international narcotics trafficking or in support of federal law enforcement efforts to interdict such trafficking. Such signals intelligence activities are subject to a separate classified annex approved earlier by the Attorney General (See Annex J to United States Signals Intelligence Directive 18). 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

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20291123~~

aids and abets such a person engaging in such activities;

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

(c) a person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power 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. Electronic surveillance within the United States targeted against communications entirely among foreign powers or between a foreign power and officials of a foreign power will be coordinated with the Federal Bureau of Investigation, including surveillances targeted against telephone communications or telecommunications that serve residential or non-official premises of a foreign power or foreign officials within the United States. This coordination is intended to satisfy the National Security Agency and the Federal Bureau of Investigation intelligence requirements, preclude duplication of effort, and ensure that appropriate minimization practices are developed and applied.

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

~~(C)~~ Illicit Communication. The term "illicit communication" means a communication transmitted in violation of the Communications Act of 1934 and regulations thereunder or of international agreements which because of its explicit content, message characteristics, or

method of transmission is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not United States persons.

(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.

~~(C)~~ International Commercial Communications. The term "international commercial Communications" means foreign communications transmitted internationally in whole or in part by one or more commercial or foreign government communications carriers, and includes, but is not limited to, [redacted] International commercial communications may be wire, telephone or radio communications transmitted by high frequency, microwave, satellite or other mode of transmission.

~~(C)~~ National Diplomatic Communications. The term "national diplomatic communications" includes all communications, regardless of the mode of transmission, transmitted by or to a foreign power and to which no United States person is a communicant. The official communications of an international organization composed of foreign governments are included in the meaning of this term, provided, however that the communications of official representatives of the United States are not included.

~~(C)~~ Selection. The term "selection," as applied to manual and mechanical processing activities, means the intentional insertion of a name, cable, TELEX, or other address and answer back or other alpha-numeric device into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

~~(C)~~ Selection Term. The term "selection term" means the composite of individual terms used to effect or defeat selection of particular communications for the purpose of interception. It comprises the entire term or series of terms so used, but not any segregable term contained herein. It applies to both mechanical and manual processing.

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

[redacted]

~~(C)~~ 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-governmental aircraft or vessel: Provided, however, that the term "U.S. person" shall not include (i) non-permanent resident aliens and entities in the United States that have diplomatic immunity as determined in accordance with Subsection 4.B; 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.

~~(C)~~ 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:

* National Diplomatic Communications;

* International Commercial Communications;

* Illicit Communications;

* 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;

* 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 Act of 1978.

Sec. 4: Procedures (U)

A. ~~(C)~~ Signals Intelligence: Communications of, or concerning, United States persons. The United States Signals Intelligence System may collect, process, retain and disseminate foreign communications that are also communications of, or concerning, United States persons. Communications of, or concerning, United States will be treated in the following manner.

1. Collection

(a) ~~(S//SI)~~ Communications of or concerning a United States person may be intercepted intentionally or selected deliberately through use of a selection term or otherwise 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, to the use of a selection term intended to intercept communications originating by or referencing that person, the National Security Agency may use such selection term to select foreign communications; 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 foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.

(b) ~~(S//SI)~~ Communications of, or concerning (1) [redacted] of a foreign power, or powers, as defined in Section 101 (a) (1) - (3) of FISA, or (2) [redacted] may be intercepted intentionally, or selected deliberately (through the use of a selection term or otherwise), upon certification in writing by the Director, NSA to the Attorney General. Such certification shall take the form of the Certification Notice appended hereto. An information copy shall be forwarded to the Deputy Secretary of Defense. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA shall advise the Attorney General and the Deputy Secretary of Defense on an annual basis of all such collection.

(c) ~~(C)~~ For purposes of the application of Parts 1, 2 and 3 of Procedure 5 (and subsection 4.A.1 (a) of this annex) to the activities of the United States Signals Intelligence System, any deliberate interception, selection or use of a selection term shall be deemed to constitute electronic surveillance; and "significant foreign intelligence" shall mean not only those items of information that are in themselves significant, but also items that are reasonably believed, based on the experience of the United States Signals Intelligence System, when analyzed together with other items, to make a contribution to the discovery of "significant foreign intelligence."

(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 deliberate selection of 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.

(2) If the United States Signals Intelligence System is intentionally collecting the communications of or concerning a non-resident alien abroad who enters the United States in circumstances that suggest that the alien is an agent of a foreign power, collection of the communications of that alien may continue for a period not to exceed seventy-two hours after it is learned that the alien is in the United States while the United States Signals Intelligence system seeks authority to continue the surveillance from the Attorney General pursuant to these procedures. [redacted]

[redacted] Communications acquired after the target is known to be in the United States, and that are not solely of, or concerning, U.S. citizens or permanent resident aliens, may be disseminated for foreign intelligence purposes until such time as diplomatic status is established or Attorney General approval is obtained. In those instances in which the diplomatic status of the alien is established, or Attorney General approval for continued surveillance is obtained, communications of, or concerning, the alien may be disseminated in accordance with subsection 4.A.4 of these procedures.

(3) If the United States Signals Intelligence System is intentionally collecting communications of, or concerning, a United States citizen or permanent resident alien abroad, it must terminate the surveillance promptly upon learning that person is in the United States. Electronic surveillance may be reinstituted only in accordance with FISA. In the event communications of, or concerning, the target continue to be collected before termination can be effected, processing and use of information derived from such communications shall be restricted to the greatest extent possible and special care shall be taken to ensure that such information is not disseminated for any purpose unless authorized in accordance with the provisions of FISA.

(e) ~~(S//SI)~~ Communications transmitted on [redacted] with a terminal in the United States that services a U.S. person may be targeted for interception upon certification in writing by the Director, NSA to the Attorney General that the target of the collection is a foreign entity and that the purpose of the collection is to obtain foreign intelligence. The certification shall take the form of the Certification Notice appended hereto. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA will advise the Attorney General on an annual basis of all such [redacted] collection. The Deputy Secretary of Defense will be provided information copies of all certifications sent to the Attorney General.

(f) ~~(S//SI)~~ Provided the proposed monitoring is not otherwise regulated by Section 4.A.1 (a)-(e), voice and facsimile communications with one communicant in the United States may be targeted for intercept only with the prior approval of the Attorney General or the Director, National Security Agency, as set forth below, unless those communications occur over channels used exclusively by a foreign power. The Director, National Security Agency, may approve the targeting of such communications if technical devices [redacted] are employed that limit acquisition by the National Security Agency to communications where the target is a non-U.S. person located outside the United States, [redacted] or to specific forms of communications used by those targets, [redacted] communications. In those cases in which it is not possible to use such technical devices, the Attorney General must approve the targeting. Approvals granted by the Director, NSA under this provision shall be available for review by the Attorney General.

(g) ~~(C)~~ [redacted] may be intercepted in accordance with Section 3 of this Annex.

Annex to Policy 1-23
Dated: 11 March 2004

(h) ~~(S//SI)~~ Use of direction finding solely to determine the location of a transmitter does not constitute electronic surveillance or collection even if directed at transmitters believed to be used by United States persons. Unless collection of the communications is otherwise authorized pursuant to this annex, the contents of communications to which a United States person is a party monitored in the course of direction finding shall be used solely to identify the transmitter.

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:

(1) When a selection term is intended to intercept a communication on the basis of encipherment or some other aspect of the content of the communication, rather than the identity of a communicant or the fact that the communication mentions a particular individual:

(a) No selection term may be used that is based on content and that is reasonably likely to result in the interception of communications to or from a United States person, or which has in the past resulted in the interception of a significant number of such

communications, unless there is reasonable cause to believe that foreign intelligence or counterintelligence will be obtained by use of such a selection term.

(b) All such selection terms shall be reviewed annually by the Deputy Director for Operations, National Security Agency, or his designee to determine whether there is reasonable cause to believe that foreign intelligence or counterintelligence will be obtained by the use of these selection terms. The review of such selection terms shall include an examination of whether such selection terms have in the past resulted in the acquisition of foreign intelligence.

(c) Selection terms based on content that have resulted or that are reasonably likely to result in the interception of communications to or from a United States person shall be designed to defeat, to the extent practicable under the circumstances, the interception of such communications not containing foreign intelligence.

(2) Foreign communications collected by the United States Signals Intelligence System or other authorized entities may be forwarded to the National Security Agency as intercepted. This applies to forwarding to intermediate processing facilities, including those of authorized collaborating centers pursuant to written agreements, provided such forwarding does not result in the production by the United States Signals Intelligence System of information in violation of these procedures.

(b) ~~(S//SI)~~ Except as provided in (b)(1), radio communications that pass over channels with a terminal within the United States must be processed by use of selection terms, unless these communications occur over channels used exclusively by a foreign power.

(1) Radio communications that pass over channels with a terminal in the United States may be processed without the use of selection terms only when necessary to determine whether a channel contains communications of foreign intelligence interest which the National Security Agency wishes to collect. Processing under this section may not exceed two hours without approval of the Deputy Director for Operations, National Security Agency, and shall in any event 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 a sufficient amount of communications of foreign intelligence interest to warrant collection and exploitation to produce foreign intelligence, additional processing of the channel must utilize selection terms.

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 Stated person is authorized if it meets 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 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)~~ Signals Intelligence: Communications of, or Concerning, Aliens and Entities [redacted]. The United States Signals Intelligence System may intentionally intercept the international communications of non-permanent resident aliens and entities in the United States [redacted]

C. ~~(C)~~ Signals Intelligence: Illicit Communications. The United States Signals Intelligence System may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning United States persons.

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;

(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)~~ Foreign Electronic Surveillance Activities. The United States Signals Intelligence System may collect information related to the conduct of electronic surveillance activities by foreign powers conducted within the United States against communications originated or intended for receipt in the United States. Collection efforts must be reasonably designed to intercept, or otherwise obtain only the results of such foreign surveillance efforts, and to avoid, to the extent feasible, the intercept of other communications. Such activities shall be conducted pursuant to orders of the United States Foreign Intelligence Surveillance Court.

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 an order from a court of competent jurisdiction) has been obtained.

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

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