All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

~~SECRET~~

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2006 DEC 13 AM 11:06

KAREN E. SUTTON CLERK

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

STANDARD MINIMIZATION

PROCEDURES FOR ELECTRONIC SURVEILLANCE

CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

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)

Classified by: Allan Kornblum, Deputy Counsel for Intelligence Operations, DOJ/OIPR
Reason: 1.5(c) and (d)
Declassify on: ~~X1 and X5~~

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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 of a nonpublic 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:

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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-CCO)~~

(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)

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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)

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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)~~

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

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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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 (i.e., 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

All redacted information exempt under b(1) and b(3). APPROVED FOR PUBLIC RELEASE

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 by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person names or identifiers and shall be limited to those selection terms reasonably likely to identify [redacted] that are authorized for intentional collection under Executive Order 12333 implementing procedures. ~~(S-CCO)~~

(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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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 other information, including that reduced to graphic or "hard copy" form such as [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)~~

(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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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:

(A) Calls to and from United States Government officials;

(B) Calls to and from children;

(C) Calls to and from students for information to aid them in academic endeavors;

(D) Calls between family members; and

(E) Calls relating solely to personal services, such as food orders, transportation, etc. ~~(S-CCO)~~

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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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, [redacted] The technical means employed shall consist of [redacted] equipment or equipment capable of identifying

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

international [redacted] or other particular international communications known to be used by the targeted foreign power and its agents. Communications to or from the target residential premises that are processed through a [redacted] of a foreign power or agent of a foreign power 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] ~~(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)~~

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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

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;

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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(i), 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)~~

(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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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:

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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;

(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;

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(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

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

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 - Collaboration with Foreign Governments ~~(S-CCO)~~

(a) The sharing or exchange of foreign communications governed by these procedures with signals intelligence authorities of collaborating foreign governments (Second Parties) may be undertaken by the NSA only with the written assurance of the Second Party that the use of those foreign communications will be subject to the retention and dissemination provisions of these procedures. ~~(S-CCO)~~

(b) Domestic communications and communications to or from United States persons shall not be shared with Second Parties. ~~(S-CCO)~~

All redacted information exempt under b(1) and b(3).

APPROVED FOR PUBLIC RELEASE

(c) Foreign plain text communications may be shared with Second Parties if they are first reviewed by NSA analysts, who shall remove references to United States persons that are not necessary to understand or assess the foreign intelligence information contained therein. ~~(S-CCO)~~

(d) Foreign enciphered or encoded communications may be shared with Second Parties without such prior review, provided that at least annually a representative sampling of those shared communications that can be deciphered or decoded is reviewed by the NSA to ensure that any references therein to United States persons are necessary to understand or assess the foreign intelligence information being disseminated. Corrective measures with respect to each target or line shall be undertaken as necessary to maintain compliance with the above dissemination standard. The results of each review shall be made available to the Attorney General or a designee. ~~(S-CCO)~~

Janet Reno
Attorney General of the United States

7/1/97
Date