

MAY 10 2002

U.S. Foreign Intelligence  
Surveillance Court

~~SECRET COMINT//XI~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE ELECTRONIC SURVEILLANCE AND : Docket Numbers: Multiple  
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :   
AND RELATED TARGETS. ~~(S)~~ :

**MOTION FOR AMENDED ORDERS PERMITTING  
MODIFIED MINIMIZATION PROCEDURES**

By this motion, the United States seeks amended orders in the above-referenced cases to permit the implementation of modified minimization procedures, under which the Central Intelligence Agency (CIA) and the National Security Agency (NSA) will be permitted to receive raw data from Court-authorized electronic surveillance and physical search; minimize such data pursuant to the minimization procedures specified herein; and retain and disseminate foreign intelligence information so obtained. The instant motion applies to surveillances and

~~SECRET COMINT//XI~~

Classified by: James A. Baker, Counsel for Intelligence  
Policy, U.S. Department of Justice

Reason: 1.5(c)

~~Declassify on: X1~~

~~SECRET COMINT//X1~~

searches conducted by the Federal Bureau of Investigation (FBI) targeting: (1) foreign powers as defined at 50 U.S.C. § 1801(a)(4); (2) agents of such foreign powers; and (3) other targets where the search or surveillance is reasonably expected to yield foreign intelligence information related to international terrorism.<sup>1</sup> However, granting the instant motion will not apply the modified minimization procedures proposed herein to the surveillances and/or searches referenced in paragraph 16 below. ~~(S)~~

In support of this motion, the United States states as follows: (U)

The Current International Terrorism Threat (U)

1. On September 14, 2001, the President of the United States declared that a national emergency has existed since September 11, 2001, "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." (U)

2. On September 15, 2001, upon the motion of the Government, the Court suspended the "Court wall," certification,

<sup>1</sup>

~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

and caveat requirements that previously had applied to Court-authorized electronic surveillance and physical search of [REDACTED] [REDACTED] related targets, while directing that the FBI continue to apply the standard minimization procedures applicable in each case. As stated in the order resulting from that motion, the Court took this action in light of, inter alia:

"the President's September 14, 2001, declaration of a national emergency and the near war conditions that currently exist;"

"the personal meeting the Court had with the Director of the FBI on September 12, 2001, in which he assured the Court of the substantial foreign intelligence purpose of the collection authority requested from this Court in the face of the nature and scope of the multi-faceted response of the United States to the above-referenced attacks;" and

"the need for the Government to rapidly disseminate pertinent foreign intelligence information to appropriate authorities."

~~(S)~~

3. On September 24, 2001, the President issued Executive Order No. 13,224, which authorized the Department of the Treasury to freeze the U.S. assets of, and prohibit U.S. persons from conducting transactions with, Usama Bin Laden, his key lieutenants, al Qaeda and related terrorist organizations, as well as entities that are known to provide financial and

~~SECRET COMINT//X1~~



~~SECRET COMINT//XI~~

operational support to al Qaeda. In so doing, the President found -

that grave acts of terrorism and threats of terrorism committed by foreign terrorists, including the terrorist attacks in New York, Pennsylvania, and the Pentagon committed on September 11, 2001, ... and the continuing and immediate threat of further attacks on United States nationals or the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and in furtherance of my proclamation of September 14, 2001, Declaration of National Emergency by Reason of Certain Terrorist Attacks, hereby declare a national emergency to deal with that threat.

(U)

Procedures Now Governing NSA and CIA Assistance (S)

4. Many of the above-captioned applications, particularly those that have been made to this Court since the terrorist attacks of September 11, 2001, contain special minimization procedures permitting the CIA, NSA, and other federal agencies to provide technical and linguistic assistance to the FBI with respect to the results of Court-authorized electronic surveillance or physical search. When NSA or CIA has provided technical or linguistic assistance pursuant to these special minimization procedures currently in use, NSA or CIA employees usually have been detailed to the FBI for the purpose of providing such assistance. Once detailed, such CIA or NSA employees have functioned as FBI employees under FBI supervision

~~SECRET COMINT//XI~~



~~SECRET COMINT//X1~~

and control. When detailed or otherwise, NSA or CIA employees who receive access to raw data<sup>2</sup> from FISA surveillances and searches pursuant to these special minimization procedures currently in use do so solely for the purpose of providing technical or linguistic assistance to the FBI. They do not retain, disseminate or make any other use of such data on behalf of NSA or CIA, unless and until the FBI disseminates information to the CIA or NSA pursuant to the FBI's standard minimization procedures. Thus, information from FBI FISA collection informs CIA or NSA intelligence reports, analyses, and assessments on international terrorism, or CIA and NSA targeting and other operational decisions, only if and when it is disseminated to CIA or NSA pursuant to the FBI's standard minimization procedures.

~~(S)~~

<sup>2</sup> Under its standard minimization procedures, the FBI is required to take certain steps to minimize the acquisition of non-foreign intelligence information. See, e.g., Section 3(c) of the procedures for electronic surveillance of a U.S. person agent of a foreign power

[REDACTED] 1  
The use of the phrase "raw data" is not meant to suggest otherwise.  
[REDACTED]

~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

Modified Procedures Proposed in this Motion (U)

5. Under the modified minimization procedures proposed herein, the CIA and NSA would be permitted to receive raw data acquired by the FBI from FISA surveillances and searches; to minimize such information pursuant to the minimization procedures proposed herein for each agency; and to retain and disseminate<sup>3</sup> foreign intelligence information consistent with such minimization procedures. Under the modified minimization procedures, CIA and NSA would be permitted to receive raw data from Court-authorized electronic surveillance and physical search from the FBI, but would not be permitted to acquire such information from Court-authorized electronic surveillance or physical search independently.<sup>4</sup> Thus, the modified minimization procedures contemplate that, at the acquisition stage,

---

<sup>3</sup> As used in this motion and the proposed NSA and CIA procedures, "dissemination" by CIA or NSA refers to any disclosure (except among NSA, CIA, and FBI personnel as described in paragraph 12 below) by CIA or NSA to a recipient who is not a CIA or NSA employee, contractor, agent or asset. ~~(S)~~

<sup>4</sup> Under Executive Order No. 12,333 (with exceptions that generally do not apply to the surveillances or searches subject to this motion), CIA is not permitted to conduct electronic surveillance or physical searches within the United States, and NSA is not authorized to conduct physical searches. Of course, as the Court is aware, NSA conducts its own Court-authorized electronic surveillances within the United States. ~~(S)~~

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

surveillances and searches would continue to be conducted solely by the FBI, without direct involvement of the CIA or NSA.<sup>5</sup> ~~(S)~~

If the Court grants this motion, it is anticipated that in some instances the FBI will continue to minimize and disseminate the foreign intelligence information from FISA surveillance or search of some targets. In some such instances, NSA and CIA may provide technical or linguistic assistance to the FBI, as previously approved by the Court. In other circumstances, CIA or NSA may take primary responsibility for processing, minimizing, and disseminating FISA collection from a particular target. If this motion is granted, in instances in which the CIA and NSA engage in further analysis of foreign intelligence information FBI initially has minimized and disseminated from raw data that would be subject to this motion, CIA and NSA also may make further disseminations in accordance with paragraph 9(b) of this motion (applicable to CIA and NSA), paragraphs 8(6) and 8(7) of this motion (applicable to NSA), and/or paragraphs 4(e) and 4(f)

---

<sup>5</sup> Where warranted by particular operational circumstances, personnel from CIA or NSA have been, and will continue to be, detailed to the FBI in order to provide technical support to the acquisition stage of a specific FISA collection. Personnel on such details are solely under FBI direction and do not report to CIA or NSA on the results of such collection, unless directed to do so by FBI and consistent with applicable minimization procedures. ~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

of Exhibit A hereto (applicable to CIA). Thus, by granting this motion the Court will provide the United States maximum flexibility to determine the appropriate application of intelligence community resources to FISA collection directed against international terrorist targets. ~~(S)~~

In support of these modified minimization procedures, the United States submits: (U)

First, the Attorney General, as defined at 50 U.S.C. § 1801(g), has adopted these modified minimization procedures, by virtue of approval of the filing of the instant motion. (U)

Second, these modified minimization procedures satisfy the requirement of the above-referenced statutory definitions that minimization procedures be

**"reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."**

50 U.S.C. § 1801(h)(1) (electronic surveillance) and § 1821(4)(A) (physical search) (emphasis added). Under the current circumstances, the foreign intelligence purposes of the above-captioned surveillances and searches encompass the detection and thwarting of planned attacks, such as those of September 11,

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

2001, as well as the provision of foreign intelligence information to the President and other national security decision-makers regarding how the United States might respond to such attacks through diplomatic, military, law enforcement, and/or intelligence activities. Timely translation, decryption, analysis, assessment, and dissemination of foreign intelligence information is essential to these purposes. Under the current circumstances, the need for expedition and thoroughness in these processes is especially acute. Congress recognized this need when it enacted Section 901 of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), Pub. L. No. 107-56, which amended 50 U.S.C. § 403-3(c) to provide that the Director of Central Intelligence, in his capacity as head of the Intelligence Community, shall "provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under [FISA] is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to [FISA] unless otherwise

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

authorized by statute or executive order" (emphasis added). Accordingly, the United States submits that it is reasonable to authorize the immediate application of all of its analytical resources to meet the prevailing need to produce and disseminate foreign intelligence information related to international terrorism, rather than permitting CIA and NSA substantive analysis to commence only after minimization, assessment, and dissemination by the FBI. Thus, the CIA and NSA should have the same ability as the FBI to produce and disseminate appropriately minimized foreign intelligence information from the raw data obtained from FISA surveillances and searches. Moreover, authorizing CIA and NSA to process raw FBI FISA data will enhance the ability of the United States to employ effectively its overseas collection capabilities against the terrorist targets.<sup>6</sup>

(S)

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

Third, these modified minimization procedures satisfy the requirement of the statutory definitions that minimization procedures

"require that nonpublicly available information, which is not foreign intelligence information as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance."

50 U.S.C. § 1801(h)(2) (electronic surveillance); § 1821(4)(B) (physical search) (emphasis added). As explained above, there are compelling reasons for the CIA and NSA to participate fully in the process whereby the United States timely identifies foreign intelligence information, assesses its importance, and ensures that appropriate action based on that intelligence can be taken. Such full participation requires CIA and NSA initially to receive United States person-identifying information as part of the raw FISA-obtained data. In applying the minimization procedures proposed herein, the CIA or NSA shall appropriately minimize United States persons' identities. ~~(S)~~

Fourth, the remaining requirements of the statutory definitions of minimization procedures at 50 U.S.C. § 1801(h) and § 1821(4) are satisfied by the CIA and NSA minimization procedures proposed herein. ~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

Fifth, because the CIA and NSA are intelligence agencies with no law enforcement authorities, the significant foreign intelligence purpose of these searches and surveillances will not be adversely affected by permitting CIA and NSA to receive the raw results of FISA collection and to disseminate information from such collection under the procedures proposed herein. Indeed, providing such raw data to these intelligence agencies reflects the significant foreign intelligence purpose of these collection activities. ~~(S)~~

FBI Processing Under Modified Procedures (U)

6. Under the modified minimization procedures, the FBI will be permitted to provide promptly to the CIA and NSA raw data from Court-authorized surveillances and searches for further processing by CIA and NSA. The FBI will also provide to the CIA and NSA the identity of the target(s) of the surveillance or search from which raw data is being provided; a statement of whether each target was identified as a U.S. person, a non-U.S. person, or a presumed U.S. person in the relevant Court pleadings or orders; a statement of what categories of non-pertinent communications and/or special or particularized minimization procedures, if any, were provided for in such pleadings or

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

order(s);<sup>7</sup> and, where applicable, a statement that the target, or any other person whose communications with an attorney are likely to be acquired through surveillance or search of the target, is known by the FBI to be under indictment.<sup>8</sup> Otherwise, the FBI's authorities regarding its handling of FISA information will not change: as it is currently, the FBI will be authorized to review such raw data, and to log, index, retain, and disseminate foreign intelligence information or evidence of crime consistent with its applicable standard minimization procedures, as well as any special or particularized minimization procedures that may apply to a particular surveillance or search. ~~(S)~~

CIA Processing Under Modified Procedures ~~(S)~~

7. Under the modified minimization procedures, the CIA will be permitted direct access to raw data from Court-authorized

---

<sup>7</sup> The FBI may provide this information by giving to NSA or CIA a copy of the relevant pleadings and/or resulting orders, or of the relevant pages thereof. ~~(S)~~

<sup>8</sup> If the FBI knows that a target or other such person is under indictment, but is prevented from disclosing that fact to CIA or NSA because of a sealing order or other legal restriction, the FBI shall not provide to CIA or NSA raw data that may include attorney-client communications of the person known to be under indictment, unless and until the matter is resolved on a case-specific basis (e.g., by having a sealing order modified so that FBI may identify the indicted person to CIA and NSA, or by presenting modified, target-specific minimization procedures to this Court). ~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

surveillances and searches. After receiving such data from the FBI, the CIA will follow the minimization procedures set out in Exhibit A hereto in its subsequent processing, retention, and dissemination of that data and information therefrom. The minimization procedures set out in Exhibit A are adapted from procedures, approved by the Attorney General and in effect in their current form since 1987, for CIA retention and dissemination of information from non-FISA electronic surveillance, including surveillance targeting United States persons abroad pursuant to Attorney General authorization under Section 2.5 of Executive Order No. 12,333.<sup>9</sup> CIA analysts are already familiar with these non-FISA procedures through training and years of experience. Thus, the United States submits that, to the extent permitted by law, CIA's application of the same standards and procedures to the raw FISA data obtained from the FBI can be expected to result in greater consistency and quality of minimization. However, since these non-FISA procedures reflect a broader definition of foreign intelligence (e.g., by including information about international narcotics activities, as such) than FISA provides in its definition of "foreign

---

<sup>9</sup> These procedures are contained in Appendix D to the Attorney General-approved Guidance for CIA Activities Conducted Outside the United States. (U)

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

intelligence information" at 50 U.S.C. § 1801(e), the categories of information that may be retained and disseminated under the procedures in Exhibit A have been narrowed from those provided in the CIA's non-FISA minimization procedures. Provisions have also been added at Paragraph 4 of the procedures at Exhibit A to address issues of heightened concern in the context of surveillances and searches within the United States (e.g., the handling of attorney-client communications). Finally, in applying these procedures, CIA expects to follow its customary practice for dissemination under Executive Order No. 12,333 and its implementing procedures regarding sanitization of U.S. person identities. This practice consists of generic substitution. Where the identity is believed necessary to understand, assess, or act on the foreign intelligence information, the identity is provided. ~~(S)~~

NSA Processing Under Modified Procedures ~~(S)~~

8. Under the modified minimization procedures, the NSA also will be permitted direct access to raw data from Court-authorized surveillances and searches. After receiving such data from the FBI, the NSA will follow its own standard FISA minimization

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

procedures,<sup>10</sup> with the modifications set out hereinbelow, in its subsequent processing, retention, and dissemination of that data and information therefrom. These standard FISA minimization procedures have been in effect in their current form since 1997. As is the case with the CIA and its own procedures, NSA analysts are already trained and experienced in these NSA FISA procedures, so that their application to the raw FISA data obtained from the FBI can be expected to result in greater consistency and quality of minimization. Certain provisions of these NSA FISA procedures are directed solely to how information may be acquired, and thus will have no application to the NSA's processing of raw FISA results it obtains from the FBI after acquisition has taken place. See, e.g., Sections 3(a), (b) and 4(a). Additionally, NSA will observe the following in applying these NSA FISA procedures to raw data from FISA searches and surveillances conducted by the FBI:

(1) References to Court-authorized electronic surveillance shall be understood to include Court-authorized physical search.

(2) References to any provision of 50 U.S.C. §§ 1801-1811 pertaining to Court-authorized electronic surveillance shall be understood to include a

---

<sup>10</sup> A copy of NSA's current standard minimization procedures for its own FISA collection is at Exhibit B. ~~(S)~~

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

corresponding provision of 50 U.S.C. §§ 1821-1829 pertaining to Court-authorized physical search.

(3) References to "communications" shall be understood to include non-communications information obtained by Court-authorized search or surveillance.

(4) The following will be added to the end of Section 3(f) of these NSA FISA procedures: "(7) OIPR shall periodically determine that information concerning communications of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act."

(5) The following will be added to the end of Section 4(b) of these NSA FISA procedures: "With respect to any other communication where it is apparent to NSA processing personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of the U.S. Intelligence Community without the prior approval of OIPR."

(6) The following will replace subsections (a), (b), and (c) of Section 8: "Nonpublicly available identity or personally identifiable information concerning United States persons may be disseminated to foreign governments, provided that:

(a) the information to be disseminated is foreign intelligence information; and

(b) the dissemination is approved by the Attorney General or approved pursuant to such procedures as the Attorney General may establish for the dissemination of such information by NSA."

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

(7) Regarding dissemination of evidence of a crime, Sections 5(a)(2) and 6(b)(8) will be superceded by the following:

"Information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12,333, and, where applicable, the crimes reporting procedures set out in the August 1995 'Memorandum of Understanding: Reporting of Information Concerning Federal Crimes,' or any successor document." ~~(S)~~

(8) NSA will also apply the following procedures:

a. 

b. 

c. Notwithstanding that the NSA standard procedures were drafted to address only surveillances, and do not expressly address the processing of non-communications information, information concerning U.S. persons that is found in non-communications information from Court-

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

authorized surveillances or searches conducted by the FBI may be retained or disseminated, but only in accordance with the standards applicable to retention and dissemination of foreign communications of or concerning U.S. persons in Section 6 of those standard NSA procedures.

Further, in applying these procedures, NSA expects to follow its customary practice of substituting in its disseminated reports a generic description for a U.S. person identity, even if that identity could appropriately be disseminated as necessary to a full understanding of foreign intelligence information. In such cases, NSA's usual practice is to provide the U.S. person's identity to a recipient of the report who specifically requests that identity in order to understand fully the disseminated foreign intelligence information. ~~(S-CCO)~~

Further Provisions Regarding CIA and NSA Processing (S)

9. In applying their respective minimization procedures, as described in paragraphs 7 and 8 above, to data from Court-authorized surveillances and searches conducted by the FBI, CIA and NSA will also:

(a) apply any special or particularized minimization procedures identified by the FBI to CIA and NSA, in accordance with paragraph 6 above, as applicable to a particular surveillance or search. As described in their respective minimization procedures at Exhibits A and B, CIA and NSA will also apply any categories of non-pertinent communications so identified by the FBI to CIA and NSA (and NSA shall apply such categories

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

instead of those listed in Section 3(f)(6) of the NSA standard FISA minimization procedures); and

(b) regard as U.S. persons any targets identified by the FBI to CIA and NSA as U.S. persons or presumed U.S. persons, in accordance with paragraph 6 above; provided, however, that if CIA or NSA, based on analysis of data from Court-authorized surveillances and searches conducted by the FBI and/or other available information, determines that a target identified by the FBI as a presumed U.S. person is properly regarded as a non-U.S. person, CIA or NSA may treat that target as a non-U.S. person for minimization purposes, and shall promptly notify the FBI and the Office of Intelligence Policy and Review (OIPR), United States Department of Justice, of such determination. For example, NSA or CIA may determine that a target identified by the FBI as a presumed U.S. person is properly regarded as a non-U.S. person upon a finding that the target is located outside of the United States, unless NSA or CIA possess specific indications that the target is a U.S. person.

Neither NSA nor CIA will be responsible for maintaining record copies of the raw data received from the FBI pursuant to this motion. ~~(S-CCO)~~

Dissemination by NSA and CIA (U)

10. Disseminations by CIA or NSA of information from FBI Court-authorized electronic surveillance or physical searches to other Federal entities will bear a legend substantively identical to the following:

"ORCON FISA INFORMATION: This dissemination includes FBI information from FBI FISA collection. Such information, and any information derived therefrom, may only be used in a U.S. legal or administrative proceeding with the advance authorization of the

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

Attorney General.<sup>[11]</sup> Any recipient interested in obtaining authorization for such use in a U.S. legal or administrative proceeding should contact FBI Headquarters.<sup>[12]</sup> Any further dissemination outside of intelligence channels and/or for law enforcement purposes must be made through FBI Headquarters. Any reproduction, dissemination, or communication (including, but not limited to, oral briefings) of this information must be accompanied by a statement of these restrictions."

~~(S)~~

11. Wherever feasible, CIA and NSA will indicate which portions of documents contain information from FBI FISA collection, so that recipients of those documents, both within and outside of CIA and NSA respectively, can determine the information to which FISA-specific restrictions apply. ~~(S)~~

12. It is anticipated that CIA and NSA will disseminate foreign intelligence information from FBI FISA collection to the full range of Federal offices and agencies with responsibilities relating to international terrorism to which CIA and NSA now

---

<sup>11</sup> The applicable statutory text requires advance authorization of the Attorney General for use in criminal proceedings, see 50 U.S.C. §§ 1806(b) and 1825(c), but the practice of successive Attorneys General has been to require authorization for use in other (e.g., immigration) proceedings also. (U)

<sup>12</sup> While a recipient interested in obtaining Attorney General authorization for use in a proceeding is directed to contact FBI Headquarters, it is anticipated that FBI Headquarters will consult with OIPR about obtaining the required Attorney General approval. ~~(S)~~

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

disseminate terrorism-related foreign intelligence from other sources. Depending on the content of a particular report, its recipients could include law enforcement agencies within the Department of Justice (e.g., the Immigration and Naturalization Service) or in other departments (e.g., the Secret Service), as well as the Criminal Division of the Department of Justice. NSA and CIA will simultaneously include FBI Headquarters in disseminations of foreign intelligence information to any Federal law enforcement agency and/or the Criminal Division of the Department of Justice. NSA and CIA will not disseminate foreign intelligence information obtained or derived from FBI FISA collection directly to any United States Attorney's Office; however, NSA or CIA may disseminate foreign intelligence information to (or otherwise call it to the attention of) FBI Headquarters, so that FBI may consider whether to disseminate such information to a United States Attorney's Office pursuant to procedures applicable to the FBI. ~~(S)~~

NSA and CIA, under their respective procedures, will also be authorized to disseminate evidence of a crime that may not be foreign intelligence information, pursuant to applicable crimes reporting procedures. See NSA procedures at paragraph 8, subparagraph (7) above; proposed CIA procedures at paragraph

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

4(f).<sup>13</sup> NSA and CIA will copy FBI Headquarters on all crimes reporting containing information from FBI FISA collection, and will also copy OIPR on crimes reporting to the Criminal Division of the United States Department of Justice that contains such information. ~~(S)~~

13. Some of the international terrorism applications to which this motion applies contain special "wall" procedures governing how the FBI discloses or disseminates information to criminal investigators or prosecutors. Generally, these special "wall" procedures require approval of such disclosures or disseminations by one or more specified officials or offices within the FBI and/or the Department of Justice; [REDACTED]  
[REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]

The instant motion will not affect the FBI's

<sup>13</sup> The current memorandum of understanding (MOU) regarding crimes reporting by intelligence agencies, including the CIA and NSA, states:

"This MOU ordinarily does not require an intelligence agency or organization to report crimes information that was collected and disseminated to it by another department, agency, or organization. Where, however, the receiving agency is the primary or sole recipient of this information, or if analysis by the receiving agency reveals additional crimes information, the receiving agency shall be responsible for reporting all such crimes information in accordance with the provisions of this MOU." (U)

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

implementation of such procedures, as they now are in effect or in whatever form they may be approved in the future. For the following reasons, the Government submits that such "wall" procedures should not apply to disseminations by NSA or CIA pursuant to the instant motion. ~~(S)~~

Most of these "wall" procedures were implemented before the enactment of the USA PATRIOT Act and were designed to ensure over time that FBI surveillances and searches continued to be conducted in furtherance of a primary foreign intelligence purpose.<sup>14</sup> In some circumstances, an unregulated flow of FISA information by FBI special agents conducting an intelligence investigation to FBI criminal investigators and/or prosecutors was thought to involve a risk that, in fact or appearance, the FISA collection was primarily serving law enforcement, rather than foreign intelligence, objectives. The disseminations to Federal law enforcement agencies or prosecutors that NSA or CIA

---

<sup>14</sup> As the Court is aware, FISA as recently amended by the USA PATRIOT Act now requires certification that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information, 50 U.S.C. §§ 1804(a)(7)(B) & 1823(a)(7)(B), and expressly authorizes consultation and coordination between Federal law enforcement officers and officers conducting FISA surveillances and searches, in order "to investigate or protect against . . . actual or potential attack or other grave hostile acts" and "international terrorism" by foreign powers and agents of foreign powers. *Id.* §§ 1806(k) & 1825(k). (U)

~~SECRET COMINT//X1~~



~~SECRET COMINT//XI~~

may make pursuant to this motion would not present the same risk. In any dissemination by, or related interaction with, NSA or CIA, neither the prosecutors nor the agents in other law enforcement agencies would have an opportunity to direct or control Court-authorized surveillance or search, because the FBI will continue to be the agency conducting the surveillance or search. (S)

Similarly, the Attorney General has approved procedures for the sharing of information from FBI intelligence investigations with criminal prosecutors. As the Court is aware, these procedures were submitted to the Court by a motion dated March 7, 2002. By an order dated April 22, 2002, the Court found that those procedures, modified in part, satisfied the definition of minimization procedures under FISA. These procedures, both as originally submitted and as modified by the Court, are directed solely at FBI dissemination of information to, and contacts with, the Criminal Division and United States Attorney's Offices. For the reasons stated above, the Government submits that no such procedures should be extended to the CIA or NSA. Of course, contacts between prosecutors and the FBI agents responsible for FISA collection will continue to be governed by procedures directed at the FBI. (S)

~~SECRET COMINT//XI~~

~~SECRET COMINT//X1~~

Scope of the Modified Procedures (U)

14. Nothing in the minimization procedures proposed herein shall be understood to authorize the CIA or NSA (i) to acquire data through Court-authorized electronic surveillance or physical search, other than by receiving from the FBI data acquired by the FBI through such electronic surveillance or physical search; or (ii) to assume law enforcement or internal security authorities or responsibilities of the FBI. The FBI, in coordination with CIA or NSA, may decide to target particular foreign powers or their agents based upon information provided by CIA or NSA. In addition, employees of the FBI, CIA, and/or NSA may work together in the review and analysis of raw data provided by the FBI to CIA and NSA pursuant to this motion (for example, to collaborate on linguistic questions; to confer on minimization-related issues; or to provide assistance from technical personnel). Such sharing of information and analysis among the FBI, CIA, and/or NSA shall not, in and of itself, be regarded as "dissemination" by CIA or NSA under the minimization procedures described herein. CIA, NSA, and FBI may also determine that they can most effectively deploy their collective expertise and resources by having one agency take primary responsibility for the analysis and

~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

dissemination of information from FISA collection regarding particular targets. ~~(S)~~

15. This motion shall apply to raw data obtained by the FBI from the above-referenced searches or surveillances since January 1, 2001. Additionally, where there is an articulable reason to believe that CIA's or NSA's receiving raw data from the above-referenced searches or surveillances that was obtained by the FBI prior to such date may further important foreign intelligence interests of the United States, CIA or NSA may also receive such raw data pursuant to the procedures described herein. Finally, it is expected that CIA or NSA will receive raw data from the above-referenced searches and surveillances when Court authority is renewed for the above-referenced searches and surveillances, as well as when authority to initiate FISA collection regarding new international terrorism targets is obtained. In cases where the Government intends to implement the procedures described herein, renewal and initial applications to this Court shall expressly reference such procedures. ~~(S)~~

16. Notwithstanding the foregoing, the instant motion will not permit CIA and NSA to have access to raw data from electronic surveillances or physical searches authorized in docket numbers providing for special minimization procedures for potentially

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

privileged information. [REDACTED]

[REDACTED] ~~(S)~~

Imminent Danger to Life (U)

17. Where a person's life or physical safety is reasonably believed to be in imminent danger, and information is relevant to the danger or its prevention, reduction, or elimination, nothing in this motion or the proposed procedures shall prohibit the CIA or NSA from:

a. retaining such information for a period of time sufficient to respond to such danger.

b. disseminating such information to any Federal officer or agency with responsibility for the matter. FBI Headquarters shall be simultaneously included in any such dissemination and notified of the other recipients of the disseminated information; however, if NSA or CIA reasonably believes that a simultaneous dissemination to FBI Headquarters would impede a sufficiently timely dissemination in response to the danger, dissemination to FBI Headquarters may be made as soon as possible after the initial dissemination.

c. making such other disseminations as reasonably may be necessary to respond to such danger, except that when practicable, any such disseminations within the United States shall be made in coordination with the FBI.

~~(S)~~

<sup>15</sup> However, the Government in the future may present to the Court modified case-specific minimization procedures that would permit CIA and NSA to have access to raw data from such electronic surveillances and physical searches. ~~(S)~~

~~SECRET COMINT//X1~~



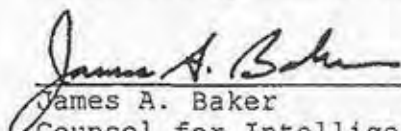
~~SECRET COMINT//XI~~

Report to Court (U)

18. Within 180 days of the implementation of the modified minimization procedures proposed herein, the United States will report to the Court on how such procedures are being implemented, and on any revisions that may be appropriate. ~~(S)~~

WHEREFORE, the United States respectfully requests that the Court issue the proposed order attached to this motion. (U)

Respectfully submitted,

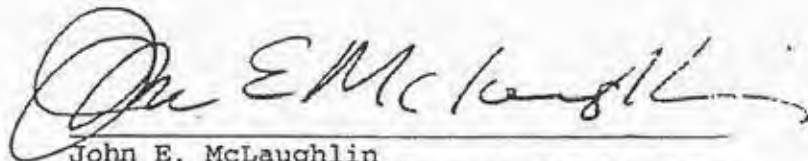
  
James A. Baker  
Counsel for Intelligence Policy  
U.S. Department of Justice

~~SECRET COMINT//XI~~

~~SECRET COMINT//X1~~

#### VERIFICATION

I have reviewed the foregoing motion and the minimization procedures set out at Exhibit A. The CIA will follow those minimization procedures, as described in the foregoing motion, with respect to information obtained from Court-authorized electronic surveillance and physical search of the above-captioned targets. ~~(S)~~



John E. McLaughlin  
Deputy Director of Central Intelligence

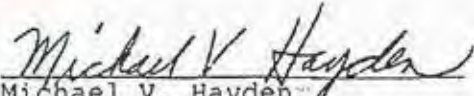
~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

### VERIFICATION

I have reviewed the foregoing motion and the NSA minimization procedures described therein. The NSA will follow those minimization procedures, as described in the foregoing motion, with respect to information obtained from Court-authorized electronic surveillance and physical search of the above-captioned targets. ~~(S)~~

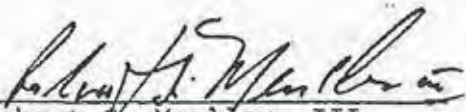
  
Michael V. Hayden  
Lieutenant General, USAF  
Director, National Security Agency

~~SECRET COMINT//X1~~

~~SECRET COMINT//X1~~

### VERIFICATION

-I have reviewed the foregoing motion and the minimization procedures described therein. The FBI will follow those minimization procedures applicable to the FBI, described in the foregoing motion, with respect to information obtained from Court-authorized electronic surveillance and physical search of the above-captioned targets. ~~(S)~~

  
Robert S. Mueller, III  
Director, Federal Bureau of Investigation

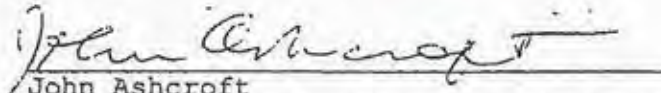
~~SECRET COMINT//X1~~



~~SECRET COMINT//X1~~

APPROVAL

I find that this motion regarding electronic surveillance and physical search of international terrorist groups, their agents, and related targets satisfies the criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978, and hereby approve its filing with the United States Foreign Intelligence Surveillance Court. ~~(S)~~

  
John Ashcroft  
Attorney General of the United States

MAY 10 2002

\_\_\_\_\_  
Date

~~SECRET COMINT//X1~~

FILED  
KAREN E. SUTTON, CLERK

MAY 10 2002

U.S. Foreign Intelligence  
Surveillance Court

~~SECRET//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

---

IN RE ELECTRONIC SURVEILLANCE AND : Docket Numbers: Multiple  
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :   
AND RELATED TARGETS. ~~(S)~~ :

---

### ORDER

This matter having come before the Court on the motion of the United States for amended orders to modify the minimization procedures in the above-captioned matters, the Court finds that the modified minimization procedures proposed in such motion have been adopted by the Attorney General, as defined under 50 U.S.C. § 1801(g), and meet the definition of minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4); and, such motion being well-founded, it is hereby GRANTED.

~~SECRET//X1~~

Derived from: Motion of the United States in the above-captioned matters.

~~Declassify on: X1~~

FILED  
KAREN E. SUTTON, CLERK

MAY 10 2002

U.S. Foreign Intelligence  
Surveillance Court

~~SECRET//X1~~

All other provisions of those orders shall remain in effect  
as originally granted or modified by prior order of this Court.

\_\_\_\_\_  
Date Filed

\_\_\_\_\_  
Time Filed

\_\_\_\_\_  
Date Approved

\_\_\_\_\_  
Time Approved

\_\_\_\_\_  
Judge, United States Foreign  
Intelligence Surveillance Court



I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. *KES*

~~SECRET//X1~~



~~SECRET//X1~~

EXHIBIT A

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

FILED  
KAREN E. SUTTON, CLERK

MAY 10 2002

U.S. Foreign Intelligence  
Surveillance Court

IN RE ELECTRONIC SURVEILLANCE AND : Docket Numbers: Multiple  
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :  
AND RELATED TARGETS. (S) :

(b)(1)

(b)(3) NatSecAct

CIA MINIMIZATION PROCEDURES FOR INFORMATION  
FROM FISA ELECTRONIC SURVEILLANCE  
AND PHYSICAL SEARCH CONDUCTED BY THE FBI

The following procedures shall apply to processing and minimization by the Central Intelligence Agency (CIA) of the raw results of electronic surveillance and physical search conducted by the Federal Bureau of Investigation (FBI) pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1811, 1821-1829 (FISA). These procedures shall be implemented as described in the Motion for Amended Orders Permitting Modified Minimization Procedures, filed with the Foreign Intelligence Surveillance Court (FISC) and captioned as above. (S)

1. As used herein, the terms "Attorney General," "foreign power," "agent of a foreign power," "United States person," "person," "foreign intelligence information," "international terrorism," and "sabotage" have the meanings specified in 50 U.S.C. § 1801. (U)

~~SECRET//X1~~

Classified by: George J. Tenet, DCI  
Reason: 1.5(c)-(d)  
Declassify on: X1

~~SECRET//X1~~

2. Information about a United States person may be retained within CIA and disseminated to authorized recipients outside of CIA if the identity of the United States person and all personally identifiable information are deleted. A generic term may be substituted which does not identify the United States person in the context of the message. If the information cannot be sanitized in such a fashion because the identity is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information, that identity may be retained or disseminated outside of CIA along with the information if:

a. The information falls within one or more of the following categories:

(1) The information indicates that the United States person has acted or may be acting as an agent of a foreign power, including information indicating that a United States person was in contact with a foreign power under facts and circumstances indicating that he intends to collaborate with a foreign power or become an agent of a foreign power;

(2) The information indicates that a United States person may be a target of intelligence activities of a foreign power;

(3) The information indicates that a United States person has engaged or may be engaging in the unauthorized disclosure of properly classified national security information;

(4) The information concerns corporations or other commercial organizations the deletion of which would hamper the correlation of foreign intelligence information on the same subject;

b. The information is enciphered or contains secret meaning;

c. The information is needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of groups engaged in international terrorism;

~~SECRET//X1~~



~~SECRET//X1~~

d. The information concerns a United States person who is or reasonably appears to be, on the basis of that or other information, an agent of a foreign power;

e. The information involves a United States person who has consented to the retention or dissemination of his communications or other information concerning him;

f. The information indicates that a United States person is engaged or may be engaged in international terrorism or activities in preparation therefor;

g. The information is needed and retained solely to identify individuals in contact with a foreign power or an agent of a foreign power (including for purposes of this subparagraph (g) any person, regardless of location, who engages in international terrorism or activities in preparation therefor; who aids, abets, or conspires with persons to engage in such activities; or who acts as a member of a group engaged in such activities);

(b)(1)

(b)(3) NatSecAct

h. [REDACTED]

i. The information concerns a person or activity that poses a threat of sabotage, international terrorism, actual or potential attack or other grave hostile act, to any facility or personnel of any agency with the Intelligence Community, or any department containing such an agency;

j. The personally identifiable information concerning the United States person is publicly available.

A communication to or from, or information about, a United States person which does not qualify for retention or dissemination in accordance with this paragraph must be destroyed. (S)

3. Nothing in paragraph 2 above shall prohibit:

a. The retention or disclosure of information necessary for the purpose of determining whether the requirements of these procedures are satisfied, provided that the recipient under

~~SECRET//X1~~



~~SECRET//X1~~

this paragraph does not retain or disclose the identity of a United States person where it is determined that the requirements of these procedures do not permit dissemination;

b. The retention of communications necessary for the maintenance of technical data bases, so long as only collection or technical personnel have access to such data bases;

c. The retention or dissemination of information concerning corporations or other commercial organizations which is limited to their identities as manufactures of equipment and related nomenclature or their locations; or

d. The retention or dissemination of information required by law to be retained or disseminated. (S)

4. CIA shall also follow the following procedures:

a. Privileged communications: As soon as it becomes apparent to CIA personnel processing a communication acquired by electronic surveillance or physical search conducted by the FBI that such communication is between a person who is known to be under criminal indictment and an attorney that represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring or processing 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, document or other material containing the privileged communication will be placed under seal and the Department of Justice, Office of Intelligence Policy and Review (OIPR) 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. With respect to any other communication where it is apparent to CIA processing personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated

~~SECRET//X1~~

~~SECRET//X1~~

within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of the U.S. Intelligence Community without the prior approval of OIPR. (S)

b. Non-pertinent Communications and Particularized Minimization Procedures: (U)

- (1) Communications determined to fall within categories of non-pertinent communications provided by the FBI to CIA regarding a particular electronic surveillance or physical search should not be retained unless they contain information that may be retained or disseminated under paragraphs 2 and 3 above. (U)
- (2) CIA processing personnel may review all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be retained or disseminated under paragraphs 2 and 3 above. (S)
- (3) Information that appears to be foreign intelligence information may be retained even if it is acquired as a part of a communication falling within a category that is generally non-pertinent. (S)
- (4) CIA processing personnel shall adhere to any special or particularized minimization procedures provided to the CIA by the FBI regarding a particular electronic surveillance or physical search. (S)
- (5) OIPR shall periodically determine that information concerning communications of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act. (S)

c. 

~~SECRET//X1~~

(b)(1)  
(b)(3) NatSecAct



~~SECRET//X1~~(b)(1)  
(b)(3) NatSecAct

d.

e. Dissemination to Foreign Governments: Nonpublicly available identity or personally identifiable information concerning United States persons may be disseminated to foreign governments, provided that the information to be disseminated is foreign intelligence information, and the dissemination is approved by the Attorney General, or approved pursuant to such procedures as the Attorney General may establish for the dissemination of such information by CIA. (S) (b)(1)  
(b)(3) NatSecAct

f. Compliance With Crimes Reporting Obligations: Notwithstanding any of the foregoing, information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12,333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (S)

~~SECRET//X1~~



~~SECRET~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

---

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)

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

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

~~SECRET~~

2

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:

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

3

- (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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

4

- (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)

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

~~SECRET~~

5

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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

6

- (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

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



~~SECRET~~

7

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] [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, 5, 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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

8

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

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

~~SECRET~~

9

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)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

10

- (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

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

~~SECRET~~

11

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]  
[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)~~

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

~~SECRET~~

12

(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-CCG)~~

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;

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



~~SECRET~~

13

- (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

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

~~SECRET~~

14

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:

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

~~SECRET~~

15

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

16

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;

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

17

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

18

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)~~

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



SECRET

19

(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

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

JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

---

IN RE ELECTRONIC SURVEILLANCE AND

PHYSICAL SEARCH OF INTERNATIONAL

: Docket Number: [REDACTED]

TERRORIST GROUPS, THEIR AGENTS,

AND RELATED TARGETS. (~~S~~)

---

ORDER

This matter is before the Court on the motion of the United States, filed by James A. Baker, Counsel for Intelligence Policy and approved by the Attorney General of the United States, to modify the minimization procedures already approved and in use in the above captioned cases since January 1, 2001; to authorize the Federal Bureau of Investigation (FBI) to disseminate to the Central Intelligence Agency (CIA) and to the National Security Agency (NSA) "raw data" (i.e. unminimized information) only where the raw data relates to international

~~SECRET~~

Classified by: Derivative

Reason: 1.5(c)

~~Declassify on: X1~~

JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

-2-

~~SECRET~~

terrorism; to include communications of or concerning United States persons collected by the FBI in electronic surveillances and physical searches authorized by this Court under the Foreign Intelligence Surveillance Act ("FISA" or the "Act"); and to allow the CIA and NSA to review, translate, analyze, minimize, use, retain and disseminate such information pursuant to supplementary minimization procedures approved by the Attorney General and filed with the Government's motion.

The Court has fully considered the matters presented including:

- a. the arguments set forth in the Government's motion and attached exhibits;
- b. the proposed supplementary minimization procedures entitled "CIA Minimization Procedures for Information From FISA Electronic Surveillance and Physical Search Conducted by the FBI," and the "Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency," as described in the Government's motion and attached exhibits, as well as the FBI's "Standard Minimization Procedures For Electronic Surveillance of A United States Person Agent Of A Foreign Power;"

~~SECRET~~



JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

-3-

~~SECRET~~

c. the supporting legal memoranda from the Office of the Deputy Attorney General dated April 5, 2002 and April 12, 2002 provided by the Government;

d. the information provided by representatives of the FBI, CIA, and NSA at a hearing on July 1, 2002, conducted on the record by the Court sitting en banc;  
and

e. the current international terrorism threat.

The Court makes the following FINDINGS:

FIRST, this Court derives its statutory powers, duties and responsibilities from the FISA;

SECOND, the FISA permits both the CIA and NSA to appear before this Court as applicant agencies seeking authorization to conduct electronic surveillances and physical searches of foreign powers and their agents;

THIRD, the FISA's legislative history recognizes that in the circumstances presented by the Government's motion, where the authorized intelligence agency is unable to process and to minimize all of the collected raw information because of linguistic or technical limitations, sharing the raw data with cooperating U.S.

~~SECRET~~

JUL 27 2001

U.S. Foreign Intelligence  
Surveillance Court

-4-

~~SECRET~~

intelligence agencies which would apply appropriate minimization procedures is permissible under FISA;

FOURTH, the proposed supplementary minimization procedures to be used by the CIA and NSA set out in the Government's motion meet the definition of minimization procedures in sections 1801(h) and 1821(4) of the FISA: AND

FIFTH, in approving minimization procedures the Court is vested by FISA with discretion to determine whether the proposed procedures are "reasonably designed" to meet their statutory purpose and to enter ex parte orders for electronic surveillances and warrants for physical searches "as requested or as modified" (50 U.S.C. § 1805(a) and (c) and § 1824(a) and (c).

Upon full consideration of the matters presented in the Government's motion, it is hereby ORDERED, pursuant to the authority conferred on this Court by the Foreign Intelligence Surveillance Act, 50 USC §§ 1801-1862, that the motion of the United States to use the aforementioned supplementary minimization procedures in all of the captioned electronic surveillances and physical searches already approved since January 1, 2001, as described in the Government's motion, is GRANTED as modified below:

~~SECRET~~



Approved for public release  
JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

-5-

~~SECRET~~

IT IS FURTHER ORDERED, that issuance of this Order does not affect in any way this Court's Order of [REDACTED]

[REDACTED]  
which order shall apply to the CIA and NSA in all disseminations and information sharing authorized herein;

IT IS FURTHER ORDERED, that use of the aforementioned supplementary minimization procedures in the future shall be subject to the approval of this Court in each electronic surveillance and in each physical search where their use is proposed by the Government as provided in 50 U.S. C. 1804(a) (5) and 1823(a) (5); and

IT IS FURTHER ORDERED, that this matter shall be fully considered again by the Court en banc at its annual conference in May of 2004. During the intervening period the Department of Justice shall provide to the Court every six months, or as otherwise directed by the Court, an informative report describing the Government's implementation of this Order by the FBI, CIA, and NSA.

~~SECRET~~



JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

-6-

SECRET

All of the members of the Court concur in this Order.

July 22, 2002

DATE

*Colleen Kollar-Kotelly*

COLLEEN KOLLAR-KOTELLY

Presiding Judge

United States Foreign Intelligence

Surveillance Court

Docket Number: [REDACTED]

SECRET

I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. */s/ [Signature]*

JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

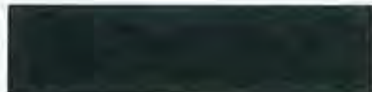
CONCURRING IN THE ORDER:

/s/

Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

*William H. Stafford, Jr.*

William H. Stafford, Jr.  
Judge, United States  
Foreign Intelligence Surveillance Court



I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. *[Signature]*

JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

CONCURRING IN THE ORDER:

*Colleen Kollar-Kotelly*

Honorable Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

*Stanley S. Brotman*

Honorable Stanley S. Brotman  
Judge, United States Foreign  
Intelligence Surveillance Court



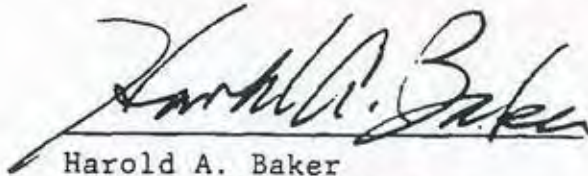
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. *[Signature]*



U.S. Foreign Intelligence  
Surveillance Court

CONCURRING IN THE ORDER:

\_\_\_\_\_  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court



Harold A. Baker  
Judge, United States  
Foreign Intelligence Surveillance Court

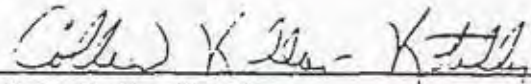


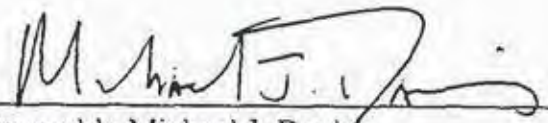
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original.

Approved for public release  
JUL 22 2002

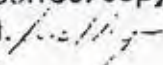
CONCURRING IN THE ORDER:

U.S. Foreign Intelligence  
Surveillance Court

  
Colleen Kollar-Koreelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable Michael J. Davis  
Judge, United States Foreign  
Intelligence Surveillance Court

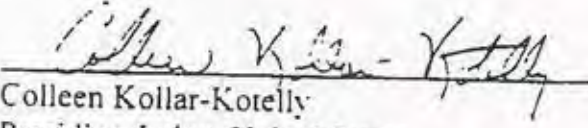


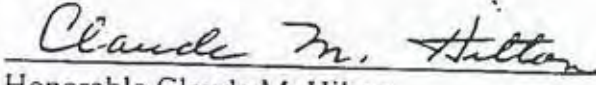
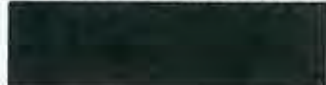
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

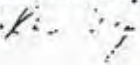
JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

CONCURRING IN THE ORDER:

  
Colleen Kollar-Koreelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable Claude M. Hilton  
Judge, United States Foreign  
Intelligence Surveillance Court  


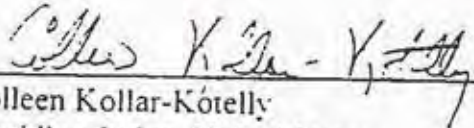
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

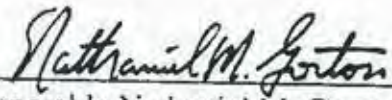


JUL 22 2002

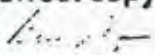
U.S. Foreign Intelligence  
Surveillance Court

**CONCURRING IN THE ORDER:**

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable Nathaniel M. Gorton  
Judge, United States Foreign  
Intelligence Surveillance Court



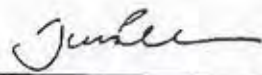
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

JUL 22 2002

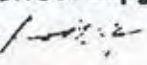
U.S. Foreign Intelligence  
Surveillance Court

CONCURRING IN THE ORDER:

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable James G. Carr  
Judge, United States Foreign  
Intelligence Surveillance Court



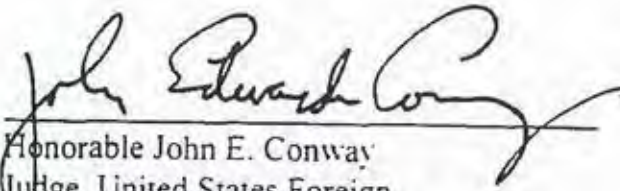
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

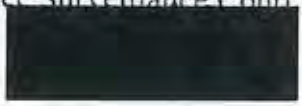
**CONCURRING IN THE ORDER:**

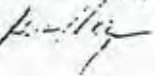
JUL 22 2001

U.S. Foreign Intelligence  
Surveillance Court

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable John E. Conway  
Judge, United States Foreign  
Intelligence Surveillance Court



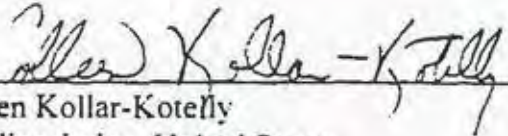
I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

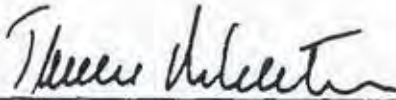
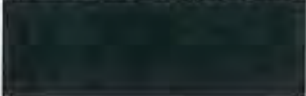


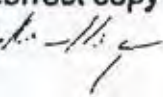
JUL 22 2002

U.S. Foreign Intelligence  
Surveillance Court

CONCURRING IN THE ORDER:

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

  
Honorable James Robertson  
Judge, United States Foreign  
Intelligence Surveillance Court  


I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

~~SECRET~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

2005 DEC 13 AM 11:06

WANE E. SUTTON  
CLERK

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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

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

FILED  
KAREN E. SUTTON, CLERK

MAY 14 2004

U.S. Foreign Intelligence  
Surveillance Court

~~TOP SECRET//COMINT//NOFORN//X1~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D. C.

---

IN RE ELECTRONIC SURVEILLANCE AND : Docket Number:   
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :  
AND RELATED TARGETS. ~~(S)~~ :

---

MOTION FOR CONTINUATION OF AMENDED ORDER

Introduction (U)

The United States of America, by counsel, hereby moves this Court, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 and 1821-1829 (FISA or the Act), to order the permanent continuation of its order of July 22, 2002, in the above-captioned matter. The United States seeks continuance of the order because it has been highly successful. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

Classified by: James A. Baker, Counsel for Intelligence  
Policy, OIPR, DOJ  
Reason: 1.4(c) - (d)  
Declassify on: X1



~~TOP SECRET//COMINT//NOFORN//X1~~

Because the order permits the rapid sharing of information within the United States Intelligence Community, the United States has obtained vital actionable intelligence regarding the activities, capabilities, plans and intentions of [REDACTED]

[REDACTED] The U.S. Intelligence Community process for sharing information - and taking action based upon such information - that the July 22, 2002 Order has fostered is now a vital part of the Nation's war on terrorism. The order has permitted the U.S. Intelligence Community to produce and disseminate to policy makers (including the President of the United States) a substantial volume of intelligence reports, and has enabled the United States and its allies to locate and apprehend numerous terrorists overseas and disrupt terrorist operations. As a result, we submit that the order has enhanced the ability of the United States Government to protect national security. Moreover, because of the manner in which the U.S. Intelligence Community has implemented the order, we submit that the intrusion on the privacy interests of Americans to date has been limited. (TS)

On July 22, 2002, the Court authorized the Federal Bureau of Investigation (FBI) to provide to the Central Intelligence Agency (CIA) and the National Security Agency (NSA) "raw data" (i.e.

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

unminimized information) obtained from certain searches and surveillances of terrorist targets under the FISA. The Court's Order, described below, modified the standard minimization procedures used in international terrorism cases. The Court further ordered that the "matter shall be fully considered again by the Court en banc at its annual conference in May of 2004." See July 22, 2002 Order at 5.<sup>1</sup> In this regard, on April 21, 2004, the Court directed that the Government:

[S]hall file a motion requesting continuation of that order. Such motion should include a statement that the factual circumstances relied upon by the Government in seeking approval of such procedures continue (or, to the extent they have changed, why the procedures should continue to be followed under current circumstances). ~~(S)~~

The United States, in support of this motion, states:

1. Prior to the July 22, 2002 Order, the CIA and the NSA provided linguistic and technical assistance to the FBI in analyzing unminimized foreign intelligence information, but could only use and disseminate limited, minimized data specifically disclosed to them by the FBI. On May 10, 2002, the Government filed a motion to provide raw data directly from the FBI to the

---

<sup>1</sup> The Court further ordered the Department of Justice to report every six months on the implementation of the Order. This motion incorporates information taken from the most recent report which covers the time period from September 1, 2003 to December 31, 2003. That report will be filed with the Court forthwith. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

CIA and the NSA, which those agencies would then minimize. The Government made this motion because of the need to

- (i) disseminate pertinent foreign intelligence information rapidly to the CIA and the NSA, (ii) enable these agencies to apply their analytical skills to the data directly, and
- (iii) provide maximum flexibility in applying Intelligence Community resources to international terrorist targets. In its Order, the Court granted the Government's motion with modifications. ~~(S)~~

2. The July 22, 2002 Order provided the following. The FBI may provide the CIA and the NSA raw data obtained from FBI electronic surveillances and physical searches targeting international terrorist groups and their agents, or from surveillances or searches of other targets where there is a reasonable expectation that the surveillance or search will reveal information related to international terrorism. The raw data provided may include communications of or information about U.S. persons. The CIA and the NSA may review, translate, analyze, minimize, use, retain and disseminate such information pursuant to certain minimization procedures. The NSA is to employ the standard FISA minimization procedures that it normally uses for conducting its Court-authorized surveillances, with certain modifications. Likewise, the CIA is to use procedures

~~TOP SECRET//COMINT//NOFORN//X1~~



~~TOP SECRET//COMINT//NOFORN//X1~~

similar to those it normally uses for the retention and dissemination of information from its non-FISA electronic surveillances, with certain modifications. ~~(S)~~

3. As described below, the FBI has successfully provided unminimized FISA information to the NSA and CIA pursuant to the Court's July 22, 2002 Order. To date, this information has consisted only of the results of Court-authorized electronic surveillance and physical searches [REDACTED]

Although

authorized by the July 22, 2002 Order, the FBI has not provided NSA or CIA with unminimized information pursuant to the Order from other means of electronic surveillance or physical searches, such as [REDACTED]. ~~(TS)~~

4. For international terrorism cases, FBI technical personnel receive and/or retrieve the data obtained from these searches and surveillances from the [REDACTED]

The FBI then forwards the data described above

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

from international terrorism searches and surveillances to the NSA and the CIA.<sup>2</sup> Before providing the data to the CIA, the FBI

(b)(1); (b)(3); (b)(7)(E)

NSA

The FBI retains the record copy of the communications. ~~(TS)~~

5. Pursuant to the Court's Order, the FBI electronically forwards to the NSA all international terrorism [REDACTED] that the FBI acquires from [REDACTED]

[REDACTED] The vast majority of the data that the NSA has reviewed was obtained from electronic surveillances and physical searches of non-U.S. person targets located outside the United States. From August 2002 to present, the NSA has issued over [REDACTED] intelligence reports based, at least in part, on raw FBI FISA data relating to international terrorism. The NSA has instructed its employees to include the caveat required by the July 22, 2002 Order on such

<sup>2</sup> As described below, the CIA generally receives data that it specifically requests, rather than the entire universe of terrorism-related [REDACTED] collected by FBI pursuant to FISA. ~~(TS)~~

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

reports.<sup>3</sup> In order to ensure that its employees comply with this requirement, the NSA includes this instruction in its FISA minimization training and also has provided its employees with written reporting guidance. ~~(TS)~~

The recipient of the raw FISA data at NSA is NSA's [REDACTED] [REDACTED] in the Data Acquisition Directorate, where it is formatted and placed in a database for analysts in NSA's Office of Counterterrorism to review. Analysts at the Office of Counterterrorism are trained by attorneys from NSA's Office of General Counsel concerning the applicable minimization procedures and the Court's July 22, 2002 Order before they are permitted access to the database containing the raw FISA data. On August 20, 2002, the Attorney General signed procedures governing the NSA's dissemination of FBI FISA information identifying U.S. persons to foreign governments, a copy of which was previously provided to the Court. ~~(S//SI)~~

6. [REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED] [REDACTED] The CIA also assists the  
FBI, at the FBI's request, with translations of communications of

<sup>3</sup> See May 10, 2002 Motion at [REDACTED]. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//X1~~



~~TOP SECRET//COMINT//NOFORN//X1~~

other international terrorism targets. The CIA receives raw FISA data from the FBI [REDACTED]

[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED] ~~(S//NF)~~

On August 20, 2002, the Attorney General signed procedures governing the CIA's dissemination of FISA information to foreign governments, a copy of which was previously provided to the Court. Those procedures apply to data processed and minimized by the CIA. They also apply to data minimized by the FBI and disseminated to the CIA where CIA engages in further analysis of the data. ~~(S)~~

[REDACTED]

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

[REDACTED]

[REDACTED] When conducting minimization reviews of NSA and CIA since implementation of the July 22, 2002 Order, OIPR has in particular focused on those agencies' handling of United States person information and, to date, has found that the agencies have acted in conformance with the applicable procedures. Thus, we have concluded that the implementation of the July 22, 2002 Order has had a limited effect on the privacy interests of U.S. persons. ~~(TS//SI)~~

8. Representatives from OIPR visit NSA and CIA to review those agencies' implementation of the Court's Order and adherence to minimization procedures. Both agencies appear to be handling the FISA data properly. OIPR expects to continue such visits on approximately an annual basis, and will continue to report to the Court every six months on the Government's implementation of the July 22, 2002 Order as required. OIPR also reviews the agencies' handling of raw data when it receives requests to initiate or renew FISA authority regarding [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] NSA reports that from August 2002 to present, approximately [REDACTED] percent of its requests for FISA authority (for the FBI to

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

conduct electronic surveillance and physical search of more than [REDACTED] have been based on information obtained through NSA's review of raw data. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In addition, the Department of Justice has submitted reports to Congress as required by law that have included discussions of the Court's July 22, 2002 Order. The Department, the FBI, CIA and NSA have briefed staff members of the Senate Select Committee on Intelligence and staff members of the House Permanent Select Committee on Intelligence on the Court's Order and on implementation thereof. ~~(TS)~~

[REDACTED]

~~TOP SECRET//COMINT//NOFORN//X1~~



~~TOP SECRET//COMINT//NOFORN//X1~~

[REDACTED]

Also in this regard, the NSA has informed OIPR that:

FBI FISA data is a critical part of NSA's mission targeting international terrorists and terrorist organizations and has yielded highly significant and very timely foreign intelligence information about [REDACTED]

[REDACTED] of international terrorist groups, [REDACTED]

It is presently the source providing the most [REDACTED]

During the last four months of 2003, FBI FISA data contributed in whole or in part to approximately [REDACTED] percent of all end product reporting from NSA's Counterterrorism Office. ~~(TS//SI//NF)~~

[REDACTED]

~~(TS//SI//NF)~~

10. The factual circumstances relied upon by the Government in seeking the initial July 22, 2002 approval to provide raw data directly to the CIA and the NSA have not changed other than those relating to the modified procedures approved by this Court in its

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

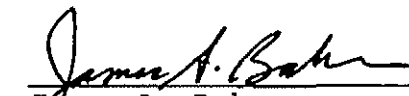
April 10, 2004 Amended Order. For this reason, the Government seeks a permanent continuation of this authority under the procedures currently in place. ~~(TS)~~

11. This motion has been reviewed for accuracy by Vito T. Potenza, Acting General Counsel, NSA; Valerie Caproni, General Counsel, FBI; and Scott W. Muller, General Counsel, CIA. (U)

WHEREFORE, the United States, by counsel, moves this Court to permit the permanent continuation of its order of July 22, 2002, in the above-captioned matter. (U)

A proposed order effecting this request accompanies this motion. (U)

Respectfully submitted,

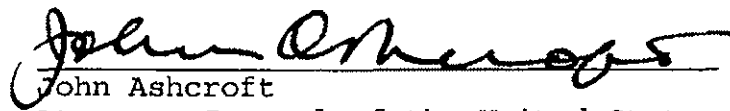
  
James A. Baker  
Counsel for Intelligence Policy  
U.S. Department of Justice

~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

APPROVAL

I find that this motion satisfies the criteria and requirements set forth in the Foreign Intelligence Surveillance Act of 1978, and hereby approve its filing with the United States Foreign Intelligence Surveillance Court. (U)

  
John Ashcroft  
Attorney General of the United States

OR

\_\_\_\_\_  
James B. Comey  
Deputy Attorney General of the  
United States

Dated: 5-13-04

~~TOP SECRET//COMINT//NOFORN//X1~~



FILED  
KAREN E. SUTTON, CLERK

~~TOP SECRET//COMINT//NOFORN//X1~~

MAY 19 2004

U.S. FOREIGN INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

---

IN RE ELECTRONIC SURVEILLANCE AND : Docket Number:   
PHYSICAL SEARCH OF INTERNATIONAL :  
TERRORIST GROUPS, THEIR AGENTS, :  
AND RELATED TARGETS. ~~(S)~~ :

---

**ORDER**

This matter is before this Court on the May 14, 2004 motion of the United States of America seeking to continue permanently the procedures approved by the July 22, 2002 Order in the above-captioned docket. Relying upon the Motion and Order issued on July 22, 2002, as well as the facts set forth in the Government's instant motion, approved for filing by the Attorney General of the United States, the Court finds that the requested permanent

~~TOP SECRET//COMINT//SI~~

Derived from: Motion to USFISC in the above-captioned  
docket number  
Declassify on: X1

~~TOP SECRET//COMINT//NOFORN//X1~~

continuation of the procedures to the July 22, 2002 Order of this Court is warranted under the facts, and that the procedures pursuant to which the National Security Agency (NSA) and the Central Intelligence Agency (CIA) will process such material meet the definition of minimization procedures set forth in 50 U.S.C. § 1801(h) and 1821(4).

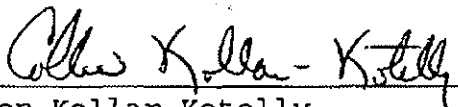
Accordingly, IT IS HEREBY ORDERED that the Federal Bureau of Investigation may continue to provide to the CIA and the NSA unminimized information obtained from searches and surveillances of terrorist targets under FISA, as set forth in the Court's July 22, 2002 Order.

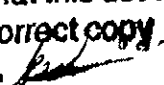
IT IS FURTHER ORDERED that all provisions of the Court's July 22, 2002 Order in docket number [REDACTED] shall remain unchanged.

Filed May 14, 2004 10:30 a.m. E.D.T.  
Date Time

Signed May 19, 2004 7:05 pm E.D.T.  
Date Time

This Order is entered with the unanimous consent of the Judges of this Court.

  
Colleen Kollar-Kotelly  
Presiding Judge, United States  
Foreign Intelligence Surveillance Court

I, Karen E. Sutton, Clerk,  
FISC, certify that this document  
is a true and correct copy  
of the original. 

~~TOP SECRET//COMINT//NOFORN//X1~~

~~SECRET~~

- 2

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:

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

3

- (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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

4

- (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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

5

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)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

6

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

7

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] [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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

8

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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

9

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)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

10

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

11

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]

[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)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

12

(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-ECG)

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;

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

13

- (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

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

~~SECRET~~

14

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:

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

15

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

15

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;

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

17

- (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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



~~SECRET~~

18

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)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

19

(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

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

~~SECRET//X1~~

EXHIBIT F

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

2006 DEC 13 AM 11:06

KAREN E. SUTTON  
CLERK

IN RE

: Docket Number:

(S):

(b)(1)

(b)(3) NatSecAct

(b)(1)  
(b)(3) NatSecActCIA MINIMIZATION PROCEDURES FOR INFORMATION  
FROM FISA ELECTRONIC SURVEILLANCE  
CONDUCTED BY NSA

The following procedures shall apply to processing and minimization by the Central Intelligence Agency (CIA) of the raw results of electronic surveillance conducted by the National Security Agency (NSA) pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1811, in the above-captioned docket number. These procedures shall be implemented as described in the application filed with the Foreign Intelligence Surveillance Court (FISC) and captioned as above. (S)

1. As used herein, the terms "Attorney General," "foreign power," "agent of a foreign power," "United States person," "person," "foreign intelligence information,"

~~SECRET//X1~~

Classified by: Michael V. Hayden, Director of the CIA  
Reason: 1.4 (c) - (d)  
Declassify on: X1



~~SECRET//XI~~

"international terrorism," and "sabotage" have the meanings specified in 50 U.S.C. § 1801. (U)

2. Information about a United States person may be retained within CIA and disseminated to authorized recipients outside of CIA if the identity of the United States person and all personally identifiable information are deleted. A generic term may be substituted which does not identify the United States person in the context of the message. If the information cannot be sanitized in such a fashion because the identity is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information, that identity may be retained or disseminated outside of CIA along with the information if:

a. The information falls within one or more of the following categories:

- (1) The information indicates that the United States person has acted or may be acting as an agent of a foreign power, including information indicating that a United States person was in contact with a foreign power under facts and circumstances indicating that he intends to collaborate with a foreign power or become an agent of a foreign power;
- (2) The information indicates that a United States person may be a target of intelligence activities of a foreign power;
- (3) The information indicates that a United States person has engaged or may be engaging in the unauthorized disclosure of properly classified national security information;
- (4) The information concerns corporations or other commercial organizations the deletion of which would hamper the correlation of foreign intelligence information on the same subject;

b. The information is enciphered or contains secret meaning;

~~SECRET//XI~~

~~SECRET//X1~~

- c. The information is needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of groups engaged in international terrorism;
- d. The information concerns a United States person who is or reasonably appears to be, on the basis of that or other information, an agent of a foreign power;
- e. The information involves a United States person who has consented to the retention or dissemination of his communications or other information concerning him;
- f. The information indicates that a United States person is engaged or may be engaged in international terrorism or activities in preparation therefor;
- g. The information is needed and retained solely to identify individuals in contact with a foreign power or an agent of a foreign power (including for purposes of this subparagraph (g) any person, regardless of location, who engages in international terrorism or activities in preparation therefor; who aids, abets, or conspires with persons to engage in such activities; or who acts as a member of a group engaged in such activities);
- h. 
- i. The information concerns a person or activity that poses a threat of sabotage, international terrorism, actual or potential attack or other grave hostile act, to any facility or personnel of any agency with the Intelligence Community, or any department containing such an agency;
- j. The personally identifiable information concerning the United States person is publicly available.

(b)(1)

(b)(3) NatSecAct

~~SECRET//X1~~



~~SECRET//X1~~

A communication to or from, or information about, a United States person which does not qualify for retention or dissemination in accordance with this paragraph must be destroyed. (S)

3. Nothing in paragraph 2 above shall prohibit:

- a. The retention or disclosure of information necessary for the purpose of determining whether the requirements of these procedures are satisfied, provided that the recipient under this paragraph does not retain or disclose the identity of a United States person where it is determined that the requirements of these procedures do not permit dissemination;
- b. The retention of communications necessary for the maintenance of technical data bases, so long as only collection or technical personnel have access to such data bases;
- c. The retention or dissemination of information concerning corporations or other commercial organizations which is limited to their identities as manufacturers of equipment and related nomenclature or their locations; or
- d. The retention or dissemination of information required by law to be retained or disseminated. (S)

4. CIA shall also follow the following procedures:

- a. Privileged communications: As soon as it becomes apparent to CIA personnel processing a communication acquired by electronic surveillance conducted by NSA that such communication is between a person who is known to be under criminal indictment and an attorney that represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring or processing 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, document or other material containing the privileged communication will be placed under seal and the Department of Justice, National Security Division (NSD) shall be notified so that appropriate

~~SECRET//X1~~



~~SECRET//XI~~

procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. With respect to any other communication where it is apparent to CIA processing personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of the U.S. Intelligence Community without the prior approval of the NSD. (S)

b. Non-pertinent Communications and Particularized Minimization Procedures  
(U)

(1) Communications determined to fall within categories of non-pertinent communications provided by NSA to CIA regarding a particular electronic surveillance should not be retained unless they contain information that may be retained or disseminated under paragraphs 2 and 3 above. (U)

(2) CIA processing personnel may review all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be retained or disseminated under paragraphs 2 and 3 above. (S)

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

(4) NSD shall periodically determine that information concerning communications of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act. (S)

c. Dissemination to Foreign Governments: Nonpublicly available identity or

~~SECRET//XI~~

~~SECRET//XI~~

personally identifiable information concerning United States persons may be disseminated to foreign governments, provided that the information to be disseminated is foreign intelligence information, and the dissemination is (i) approved by the Attorney General, or (ii) approved pursuant to such procedures as the Attorney General may establish for the dissemination of such information by CIA. In addition, to the extent authorized by the Director of the Central Intelligence Agency (DCIA) and in accordance with DCIA directives, CIA may make such disseminations without specific Attorney General approval subject to the following procedures: (S)



(b)(1)  
(b)(3) NatSecAct

~~SECRET//XI~~



~~SECRET//X1~~

(3) CIA will make a written record of each dissemination approved pursuant to these procedures, and information regarding such disseminations and approvals shall be made available for review by the NSD on at least an annual basis. (S)

- d. Compliance With Crimes Reporting Obligations: Notwithstanding any of the foregoing, information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12,333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (S)

~~SECRET//X1~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT AUG 26 PM 3:53

WASHINGTON, D.C.

KAREN SUTTON  
CLERK

IN RE DNI/AG 702(g) CERTIFICATION

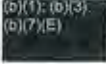
(b)(1), (b)(3), (b)(7)(E)

~~(S)~~

~~UNDER SEAL~~

Docket No. 702(i)-08-01

GOVERNMENT'S PRELIMINARY RESPONSES TO  
CERTAIN QUESTIONS POSED BY THE COURT ~~(S)~~

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits its preliminary responses (attached hereto at Tab 1) to certain of the questions previously posed by this Court regarding DNI/AG 702(g) Certification  and the targeting and minimization procedures submitted therewith. The Government reserves the right to supplement and/or modify these responses as appropriate during the hearing scheduled in the above-captioned matter on August 27, 2008.

(b)(6)



National Security Division  
United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by: Matthew G. Olsen, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: ~~26 August 2033~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

**1. How is the mechanism permitting National Security Agency (NSA) to target additional foreign powers not listed in Exhibit F consistent with the statutory requirement that the Director of National Intelligence and Attorney General certify that a significant purpose of the acquisition is to acquire foreign intelligence information? (S)**

- In [REDACTED] the Attorney General and Director of National Intelligence authorized the acquisition of foreign intelligence information concerning all foreign powers that meet the statutory definitions in: (S)



- There are a number of constraints that operate in concert to ensure, as certified by the Attorney General and Director of National Intelligence, that a significant purpose of the acquisition is to acquire foreign intelligence information. (S)
  - First, NSA cannot target "consistent with this certification non-United States persons reasonably believed to be located outside the United States" unless NSA determines that the target "possesses and/or is likely to communicate foreign intelligence information" as defined by 50 U.S.C. § 1801(e). (S)
  - Second, the "foreign intelligence information" to be acquired by such targeting must concern a group that is a "foreign power" as defined by 50 U.S.C. § 1801(a) [REDACTED]<sup>1</sup> (S)

<sup>1</sup> Indeed, the concept of "foreign power" is itself integral to the "foreign intelligence information" definitions in 50 U.S.C. § 1801(e). See, e.g., 50 U.S.C. § 1801(e)(1)(A) ("Foreign intelligence information" means information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect

~~TOP SECRET//COMINT//ORCON,NOFORN~~

|                |                                                               |
|----------------|---------------------------------------------------------------|
| Classified by: | Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ |
| Reason:        | 1.4 (c)                                                       |
| Declassify on: | <del>26 August 2033</del>                                     |



~~TOP SECRET//COMINT//ORCON,NOFORN~~

○



●



○



●



- NSA targeting procedures require that the foreign intelligence purpose of each tasking be documented. (S)
- One aspect of the oversight reviews conducted by the Office of the Director of National Intelligence and the Department of Justice is to check that such documentation exists. (S)

against . . . actual or potential attack or other grave hostile acts of a *foreign power* or an agent of a foreign power.").

(emphasis added.) (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

- In doing those checks, [REDACTED] for which notice had not been given would be discovered and subject to review. ~~(S)~~

**2. The Court had several questions concerning the "abouts" collection and the IP filters used to effect that collection. ~~(TS//SI)~~**

**First, which person is being "targeted" in the abouts collection? Is it still the user of the selector? Or is it one or both of the communicants of the message containing the reference to the selector? ~~(TS//SI)~~**

- In cases where NSA seeks to acquire communications that refer to a selector used by a target that are not to and from the selector used by the target, the person being "targeted" is the user of the selector. ~~(TS//SI)~~
- Viewing the "target" of the abouts collection as the user of the tasked selector is most consistent with the statutory language: ~~(TS//SI)~~
  - Under 702(a), the AG and DNI can authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." ~~(TS//SI)~~
    - ◆ A person is "targeted" by tasking an electronic communications [REDACTED] ("selector") that he uses. ~~(TS//SI)~~
    - ◆ By virtue of operation of the targeting procedures, the tasked selector is believed to be used by a non-United States person reasonably believed to be located outside the United States. ~~(TS//SI)~~
  - The purpose of acquiring a communication containing a reference to a selector used by a target is to acquire foreign intelligence information about the target – regardless of whether the communication was sent to or from a selector used by the target. ~~(TS//SI)~~
    - ◆ This is reflected in the NSA targeting procedures: namely, the "abouts" collection involves "cases where NSA seeks to acquire communications about the target that are not to or from the target." ~~(TS//SI)~~
    - ◆ So, the focus of the abouts collection remains "the target," even though communications that are not sent to or from "the target" are acquired. ~~(TS//SI)~~
  - Further, the operation of the Internet Protocol (IP) address filters [REDACTED] [REDACTED] prevents the intentional acquisition of communications "about" the target as to which the senders and all intended recipients are known at the time of acquisition to be located in the United States. ~~(TS//SI)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- Thus, operation of the targeting procedures ensures that the abouts collection targets non-US persons reasonably believed to be located outside the United States and prevents the intentional acquisition of communications about the target as to which the senders and all intended recipients are known at the time of acquisition to be located in the United States. (TS//SI)
- Furthermore, any United States person information that is incidentally acquired through the abouts collection will be treated in accordance with the minimization procedures adopted for the certification. (TS//SI)
- It is also possible to conceptualize that the foreign-based, non-US person sender or recipient of the abouts communication may also be a "target." (TS//SI)
- The Government previously took a similar position with respect to the certifications executed under the Protect America Act of 2007 (PAA): "The person from whom NSA seeks to acquire communications in such cases is the party to the communication who is reasonably believed to be located outside the United States." However, that position was in many respects a function of the statutory language of the PAA: (TS//SI)
  - ◆ 105B(a) -- the abouts collection was for the purpose of acquiring "foreign intelligence information concerning a person reasonably believed to be located outside the United States" (i.e., the user of the tasked selector). (TS//SI)
  - ◆ 105A -- the abouts collection was not "electronic surveillance" because it was "directed at a person reasonably believed to be located outside the United States." (TS//SI)
- However, this interpretation is less satisfactory under the new statute, which contains no requirement that the acquisition be "directed at" a person reasonably believed to be located outside the United States. (TS//SI)
  - ◆ To the extent that the targeting procedures retain the "directed at" language, it is for the purpose of making clear that that the "target" is in no event a person located in the United States. (TS//SI)

**Second, what has NSA's experience been with the IP filters? Have they been effective in limiting the collection to communications with at least one communicant located outside the United States?** (TS//SI)

- Yes, they have been effective in limiting the collection to communications with at least one communicant located outside the United States. NSA is not aware of a case where an about collection resulted in the acquisition of a communication where both ends were inside the United States. (TS//SI)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

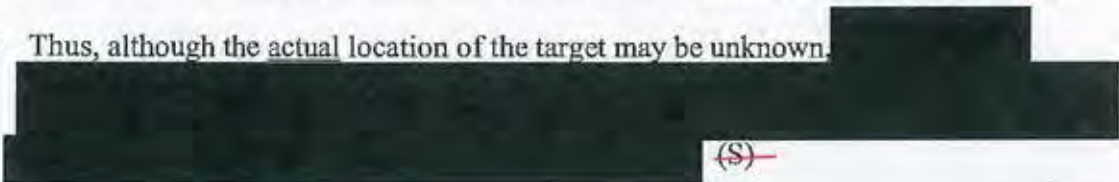


~~TOP SECRET//COMINT//ORCON,NOFORN~~



3. The Court wants to know why the presumption reflected in the third paragraph of the subsection dealing with the assessment of the non-US person status of the target is reasonable as a general matter and in particular when the location of the individual is unknown. The Court also wants to know what measures are taken to locate information that could otherwise undermine the presumption.

- It is important to note that the use of the presumption is only one aspect of a broader range of information upon which a targeting determination is made. Targeting decisions under the targeting procedures are made "in light of the totality of the circumstances based on information available with respect to [the new target]." (S)
- Thus, although the actual location of the target may be unknown.



- In such an instance, the actual location of the recipient/new target is unknown. (S)
- As this Court has recognized, it is reasonable to presume that a non-US person located overseas communicates most frequently with other, non-United States persons overseas. (S)
- "This Court sees no reason to question the presumption that the vast majority of persons who are located overseas are not United States persons and that most of their communications are with other, non-United States persons, who are also

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

located overseas." Mem. Op. and Order, In re DNI/AG Certification 

 at 87 (FISA Ct. Jan. 15, 2008). ~~(S)~~

- "This *common sense presumption* is embodied in the Department of Defense procedures governing the collection of information about United States persons, which state, 'a person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.'" *Id.* at 87 n.81 (emphasis added). ~~(S)~~
  - ◆ The presumption contained in the NSA targeting procedures is roughly the same as the "common sense presumption" quoted by the Court.  ~~(S)~~
  - ◆ The presumption is also contained in the NSA FISA Standard Minimization Procedures, which were adopted by Attorney General Reno in 1997 and which have been used in numerous NSA FISA applications approved by the Court since that time. ~~(S)~~
  - Thus, although the actual location of the new target may unknown in a particular instance, NSA may reasonably believe, based on the totality of the circumstances, that the new target is located overseas and, therefore, may be presumed to be a non-United States person. ~~(S)~~
  - NSA takes several steps designed to locate any information in its possession that would undermine the presumption: ~~(S)~~
- 

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

4. Section I. of the targeting procedures lists [REDACTED] types of information that NSA analysts examine when making a foreignness determination — [REDACTED]

(S)

- In addition, a second level of review takes place prior to tasking, which includes a review of the tasking analyst's basis for reasonably believing the target is located outside the United States and the source document(s) supporting that reasonable belief. (S)

5. The discussion of the post-targeting analysis done by NSA describes the [REDACTED] checks as being done "routinely." Are those checks done for each targeted selector? How often are those checks done? What criteria does NSA employ to determine if and/or how often such checks should be done? (S)

- The checks are done for each selector. (S)

• [REDACTED]

(S)

• [REDACTED]

(S)

6. The discussion of the post-targeting analysis done by NSA says that [REDACTED]

[REDACTED] The Court wants to know, in practice, how often such analysis is done. (S)

• [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

- In all cases, analysts remain responsible for following their target's locations and for the validity of continued acquisition of information regarding that target. ~~(S)~~

**7. In the Documentation section, there's no requirement that NSA document the source(s) of the information containing the information upon which NSA determined that the target is a non-US person. Was that inadvertent or intentional? ~~(S)~~**

- The omission of this requirement was intentional, for the following three reasons: ~~(S)~~
  - First, the cited source of the information upon which the foreignness determination for the target was based may also contain information bearing on the non-US-person status of the target, making a separate citation unnecessary. ~~(S)~~
  - Second, oftentimes the basis for NSA's determination that a target is a non-US person rests on the reasonable presumption, discussed above, that [REDACTED]  
[REDACTED] Inasmuch as the targeting procedures already require citations to the sources of information upon which a foreignness determination is based, a separate citation to those same sources would be unnecessary. ~~(S)~~
  - Third, checks to determine whether a selector has been used from the United States are required in all cases; thus, requiring a notation that a check was done in each case would be unnecessary. ~~(S)~~

**8. The noncompliance reporting requirement doesn't include a requirement that the intentional targeting of a US person be reported (though information acquired as a result of such targeting is required to be purged). The Court wants to know why. The reporting requirement also focuses more narrowly on noncompliance incidents involving improper tasking decisions rather than all types of noncompliance incidents. The Court wants to know why. ~~(S)~~**

- The failure to include the reporting of intentional targeting of U.S. person was an oversight. ~~(S)~~
- Intentional tasking of a U. S. person is an incident of noncompliance and will be reported to DOJ, ODNI OGC and ODNI CLPO within 7 days of NSA learning of such an incident. ~~(S)~~
- The reporting requirement focuses on improper tasking decisions, rather than all types of noncompliance incidents, because there are types of purely "technical" incidents of noncompliance that do not result in a tasking decision that is inconsistent with the statute. These "technical" incidents of noncompliance are often discovered during

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

routine oversight visits. Further, as these "technical" incidents are identified, corrective action is taken (e.g., a previously omitted source citation is added to the tasking documentation). ~~(S)~~

- NSA fully intends to discuss all issues of noncompliance with its procedures with DOJ and DNI representatives during routine oversight visits, which are intended to take place at least every 60 days. ~~(S)~~

**9. With respect to Section 3(b)(4) of the NSA minimization procedures, the first sentence is written in the passive voice. The Court wants to know who makes the determination discussed in that sentence. The Court also wants to know what the "such communications" in the second sentence refers to. ~~(S)~~**

- The intelligence analyst makes the determination. ~~(S)~~
- "Such communications" refers to communications containing foreign intelligence or evidence of a crime. ~~(S)~~

**10. Generally, why is the five years retention period in the NSA minimization procedures reasonable? ~~(S)~~**

- The nature of NSA's foreign intelligence targets, particularly regarding its counterterrorism targets, is such that it can take data gathered over an extended period of time may be required to understand its foreign intelligence value and to connect seemingly unconnected things. ~~(S)~~
- This retention period has appeared in other minimization procedures approved by the Court (e.g., docket numbers [REDACTED] and [REDACTED]). ~~(S)~~

**11. With respect to Section 5 of the NSA minimization procedures, can the Director of NSA delegate the decision making required by this provision? ~~(S)~~**

- The decision may be made by the Director of NSA or the acting Director of NSA only. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

12. The penultimate sentence of the Federal Bureau of Investigation (FBI) minimization procedures included as Exhibit D to the certification states: "The FBI will implement these non-U.S. Person Standard Minimization Procedures, as modified above, in accordance with FBI Policy Directive No. 0100N (effective June 30, 2008) as appropriate." (emphasis added.) What is the meaning of "as appropriate" in this sentence? Will the "case ownership" model reflected in the policy generally (through the designation of "case coordinators"), and the provisions of the policy directive applicable to (b)(1); (b)(3); (b)(7)(E) cases in particular, be applied to unminimized communications obtained by the FBI? (S)

- The addition of "as appropriate" to the end of the sentence above is intended to reflect that only certain provisions of FBI Policy Directive No. 0100N may be applicable to information acquired pursuant to section 702 of the Act. (S)
- Specifically, the most pertinent provision of the policy directive is Section 10, which concerns information acquired (b)(1); (b)(3); (b)(7)(E). (S)
- If read narrowly, Section 10 could be interpreted not to apply here, because acquisitions under section 702 of the Act are not, strictly speaking, (b)(1); (b)(3); (b)(7)(E).
- However, because acquisitions conducted under section 702 of the Act are similar to (b)(1); (b)(3); (b)(7)(E) it is "appropriate" that Section 10 apply to information acquired under section 702 of the Act. Section 10 expressly requires the designation of case coordinators who shall be responsible for such information. (S)
- Furthermore, Section 10 itself expressly exempts (b)(1); (b)(3); (b)(7)(E) from a number of other provisions of the policy directive. Those same exemptions would apply to acquisitions conducted under section 702 of the Act. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

13. The NSA minimization procedures included as Exhibit B to the certification require that a determination by the Director of NSA to retain certain types of information must be made in writing. The CIA minimization procedures included as Exhibit E to the certification likewise require the Director of the CIA to make such a determination in writing. However, although the FBI minimization procedures attached as Exhibit D to the certification require that such a determination must be made by the Director of the FBI, that determination is not required to be in writing. Was the omission of that requirement from the FBI minimization procedures intentional and, if so, for what purpose was that requirement omitted? ~~(S)~~

- The omission of an express requirement that the FBI Director must determine in writing that certain types of information may be retained was not intended to suggest that the process by which the FBI Director reaches that determination would be any less rigorous than that of the Director of NSA or the Director of the CIA. ~~(S)~~
- The FBI has represented that any such determination by the Director would be made in writing, even if not expressly required by the minimization procedures. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

28 PH 6:11  
CLERK

IN RE DNI/AG 702(g) CERTIFICATION

(b)(1), (b)(3), (b)(7)(E)

~~UNDER SEAL~~

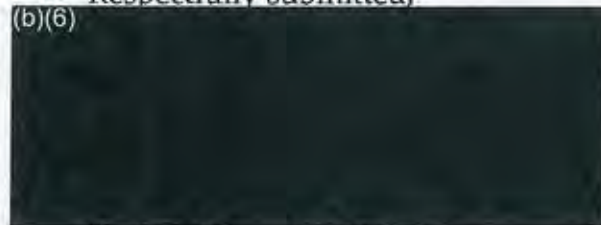
Docket No. 702(i)-08-01

NOTICE OF FILING (S)

NOTICE IS HEREBY GIVEN that the United States of America, through the undersigned Department of Justice attorney, submits its analysis of 50 U.S.C. § 1806(i) (attached hereto at Tab 1).

Respectfully submitted,

(b)(6)



National Security Division  
United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~Classified by: Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ~~  
~~Reason: 1.4(c)~~  
~~Declassify on: 27 August 2033~~

~~SECRET~~

Approved for public release

**Question:** Whether 50 U.S.C. 1806(i) requires that the Attorney General find that information acquired from a person targeted under section 702 of FISA while that person, reasonably believed to be outside the United States, is in the United States "indicates a threat of death or serious bodily harm" before the National Security Agency may retain such information. (U)

**Answer:** No. Because NSA has intentionally acquired the information, section 1806(i) does not apply and NSA may retain the information without such a determination. ~~(S)~~

- Under section 702 of FISA, as amended, the Attorney General and the Director of National Intelligence "may authorize jointly . . . the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information." (U)
- The reasonable belief standard allows for an inadvertent erroneous determination of location and recognizes that a target's location may change before the Government learns of the movement. (U)
- Of course, the reasonable belief standard (as well as separate provisions of section 702) preclude the Government from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," section 702(b)(2), and from "intentionally acquir[ing] any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States," section 702(b)(4). (U)
- Thus, provided that, at the time of the acquisition, the target was reasonably believed to be outside the United States (and thus not "known" to be here), the acquisition is authorized by section 702. (U)
- Subsection 1806(i) provides no limitation on the use of the information because the NSA's acquisition remains intentional even where the target is mistakenly, but reasonably, believed to be outside the United States. ~~(S)~~
- Subsection 1806(i) provides that "[i]n circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person." (U)

~~SECRET~~

|                |                                                               |
|----------------|---------------------------------------------------------------|
| Classified by: | Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ |
| Reason:        | 1.4(c)                                                        |
| Declassify on: | 27 August 2033                                                |



~~SECRET~~

Approved for public release

- The provision originally covered only radio communications, but was recently amended to cover all communications to make it technology neutral. See 154 Cong. Rec. S6133 (daily ed. June 25, 2008). (U)
- The plain language of subsection 1806(i) demonstrates that it only applies to “unintentional acquisition[.]” (U)
  - The legislative history of this provision as originally enacted indicates that it was meant to restrict the Government’s use of **unintentionally acquired** private domestic radio communications. Congress concluded that section 1806(i) was needed because “electronic surveillance” of radio communications, as defined in section 1801(f)(3), covered only the intentional acquisition of the contents of private domestic radio communications. Members had expressed concern that unless the use of **unintentionally acquired communications** was restricted, the Government might sidestep FISA by acquiring domestic communications without **intentionally targeting any particular communication**. Subsection 1806(i) minimized this possibility by restricting the use of any information acquired in this manner to only the gravest of circumstances, i.e., where the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person. H. Rep. 95-1283 (June 8, 1978) at 94. (U)
  - The legislative history also suggests that subsection 1806(i) was intended to address the risk inherent in radio collection of intercepting domestic communications. S. Rep. 95-701 (Mar. 14, 1978) at 36. (“Thus, intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of communications intended to be totally domestic.”) (U)
- In contrast, the NSA’s acquisition, which targeted a person reasonably believed to be outside the United States, is intentional and remains so even if the person has, unbeknownst to the NSA, moved here. ~~(S)~~
- Thus, section 1806(i) simply does not apply to information acquired under section 702 when the target, who is reasonably believed to be outside the United States is, in fact, here. (U)
- Accordingly, the domestic communications carve-out in the minimization procedures adopted by the Attorney General in consultation with the Director of National Intelligence in DNI/AG 702(g) Certification (b)(1); (b)(3); (b)(7)(E) which is intended to apply to domestic communications acquired after a target has entered the U.S. but before NSA knows that the target has entered the U.S., is consistent with section 1806(i). ~~(S)~~
- Section 1806(i) would apply, however, to unintentional acquisitions under section 702(a) such as a circumstance where a selector appropriate for targeting under section 702(a) was incorrectly identified to an electronic communications service provider (e.g., as a result of a typographical error) or where a technical error resulted in the acquisition from

~~SECRET~~



~~SECRET~~

Approved for public release

a non-targeted selector. ~~(S)~~

- In those circumstances, the acquisition of the content of a communication would be accidental and unintentional. ~~(S)~~
- In addition, that the acquisition is authorized by section 702 (under the reasonable belief standard) renders inapplicable section 109's general prohibition on "the disclo[ure] or use [of] information obtained under color of law by electronic surveillance" with the knowledge or the reason to know "that the information was obtained through electronic surveillance not authorized by this Act . . ." (even assuming that the section 702 acquisition would constitute electronic surveillance). (U)
  - The electronic surveillance would indeed be "authorized by this Act" where the target was reasonably, even if mistakenly, believed to be outside the United States. (U)

~~SECRET~~

~~SECRET//COMINT//NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

SEP 2 PM 1:36  
CLERK

IN RE DNI/AG 702(g) CERTIFICATION

(b)(1); (b)(3); (b)(7)(E)

~~UNDER SEAL~~

Docket No. 702(i)-08-01

NOTICE OF CLARIFICATION AND CORRECTION (U)

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, submits the following clarifications and corrections related to certain documents previously submitted to this Court in the above-referenced matter: (U)

I. CLARIFICATIONS (U)

National Security Agency (NSA) Targeting Procedures ~~(S)~~

1. The second paragraph under the heading "Assessment of the Non-United States Person Status of the Target" on page 4 of NSA's targeting procedures, provides:

~~(S)~~ Furthermore, in order to prevent the inadvertent targeting of United States persons, NSA [REDACTED]

[REDACTED]

~~SECRET//COMINT//NOFORN~~

Classified by: Matthew G. Olsen, Deputy Assistant  
Attorney General, NSD, DOJ  
Reason: 1.4(c)  
Declassify on: ~~1 September 2033~~



~~SECRET//COMINT//NOFORN~~



The term inadvertent, as used in this provision of the NSA targeting procedures, refers to the erroneous determination of the non-United States person status of a target. This provision of the targeting procedures does not implicate 50 U.S.C. § 1806(i), because the provision relates to the U.S. person status of the target and not whether the acquisition by NSA was intentional or unintentional. (S)—

2. The fifth paragraph under the heading "IV. (U) OVERSIGHT AND COMPLIANCE" on page 9 of the NSA's targeting procedures, provides:

~~(S)~~ In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

1. Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA **inadvertently** acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures. (emphasis added) ~~(S)~~

The term "inadvertently," as used in this provision of the NSA targeting procedures, refers to the erroneous determination of the location of the target. The term does not refer to NSA's decision to target a person reasonably believed to be outside the United States to acquire foreign intelligence information under section 702 of FISA.

~~SECRET//COMINT//NOFORN~~



~~SECRET//COMINT//NOFORN~~

As noted in the Government's section 1806(i) analysis submitted to this Court on August 28, 2008, under section 702, the Attorney General and the Director of National Intelligence "may authorize jointly . . . the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information." This reasonable belief standard allows for an inadvertent erroneous determination of location and recognizes that a target's location may change before the Government learns of the movement. The reasonable belief standard (as well as separate provisions of section 702) preclude the Government from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," section 702(b)(2), and from "intentionally acquir[ing] any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States," section 702(b)(4). Thus, provided that, at the time of the acquisition, the target was reasonably believed to be outside the United States (and thus not "known" to be here), the acquisition is authorized by section 702. Section 1806(i) provides no limitation on the use of the information because the NSA's acquisition remains intentional even where the target is mistakenly, but reasonably, believed to be outside the United States. ~~(S)~~

National Security Agency Minimization Procedures ~~(S)~~

3. Section 3(b)(1) of the NSA's minimization procedures at page 3 provides:

Personnel shall exercise reasonable judgment in determining whether information acquired must be minimized and shall destroy inadvertently

~~SECRET//COMINT//NOFORN~~

~~SECRET//COMINT//NOFORN~~

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 acquisition (e.g., the communication does not contain foreign intelligence information); or, as containing evidence of a crime which may be disseminated under these procedures. Inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. ~~(S//SI)~~ (emphasis added)

This provision relates to minimization and does not implicate section 1806(i).

Section 3(a), which immediately precedes section 3(b)(1), imposes a general requirement to conduct the authorized acquisition in "a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition." Section 3(b)(1) relates to the minimization of communications of or concerning U.S. persons that are neither relevant to the foreign intelligence purpose of the acquisition nor evidence of a crime. ~~(S//SI)~~

The phrase "inadvertently acquired" in this context refers to an acquisition of such a communication notwithstanding reasonable steps taken "to minimize the acquisition of information not relevant to the authorized purpose of the acquisition." In this connection, the "inadvertence" does not relate to the intentional or unintentional character of the acquisition as described in the Government's analysis of section 1806(i). Nor does it relate to the correctness of the Government's belief that the target is a non-U.S. person located overseas. The minimization requirement of section 3(b)(1) applies

~~SECRET//COMINT//NOFORN~~



~~SECRET//COMINT//NOFORN~~

equally to all communications acquired and retained by the Government — whether the collection is intentional or unintentional, and without regard to the correctness of the Government's belief as to the location or U.S. person status of the target. ~~(S//SI)~~

For example, this provision would apply with equal force to: (i) a communication unintentionally acquired based on a typographical error but retained in the discretion of the Attorney General pursuant to section 1806(i) because the contents indicates a threat of death or serious bodily harm; (ii) a communication intentionally acquired pursuant to section 702(a) where the sender and all intended recipients are in fact located in the U.S. at the time of acquisition, but where the Government did not know at the time of acquisition that it was intentionally acquiring a purely domestic communication, which is retained in the discretion of the Director of the NSA for any of the reasons provided in section 5 of the NSA's minimization procedures; and (iii) a foreign communication of a non-U.S. person intentionally acquired pursuant to section 702(a). In sum, the use of the phrase "inadvertently acquired" in section 3(b)(1) of the NSA's minimization procedures relates strictly to minimization, and does not implicate section 1806(i). ~~(S//SI)~~

4. Section 3(b)(6) of the NSA's minimization procedures at page 4 provides:

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//SI)~~ (emphasis added)

~~SECRET//COMINT//NOFORN~~



~~SECRET//COMINT//NOFORN~~

The term "inadvertently," as used in this provision of the NSA minimization procedures, refers again to the erroneous determination of the location of the target. Accordingly, for the same reasons set out in paragraph 2 above, NSA's acquisition is authorized by section 702 and section 1806(i) provides no limitation on the use of the information, because the NSA's acquisition remains intentional even where the target is mistakenly, but reasonably, believed to be outside the United States. ~~(S)~~

## II. CORRECTIONS

### National Security Agency Minimization Procedures ~~(S)~~

5. At Tab 1 to this Notice, the Government respectfully submits a substitute page 3 of the NSA minimization procedures for the purpose of correcting two typographical errors found in paragraph 3(b)(1). The corrections include: (a) adding the word "not" in the sixth line of paragraph 3(b)(1) between the words "as containing"; and (b) replacing the misspelled word "Inadvertantly" with its correct spelling – "Inadvertently" – in line 7 of the paragraph. ~~(S//SI)~~

### Federal Bureau of Investigation Minimization Procedures ~~(S)~~

6. At Tab 2 to this Notice, the Government respectfully submits a substitute first page to the FBI minimization procedures for the purpose of correcting the following typographical error: the removal of the included word "not" between the words "is a" in the last line of paragraph b.1. ~~(S//NF)~~

~~SECRET//COMINT//NOFORN~~