

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

APPROVED FOR PUBLIC RELEASE

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

207 APR -4 PM 5:19

WASHINGTON, D. C.

CLERK

IN RE

:

: Docket Number:

:

(S):

ORDER

The United States of America has applied, pursuant to section 105(e)(2), 50 U.S.C. § 1805(e)(2), of the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 ("FISA" or "the Act"), for an extension of the orders issued in the above-captioned docket number (hereinafter "application for an extension").

The Court has given full consideration to the matters set forth in the Government's application for an extension and finds as follows:

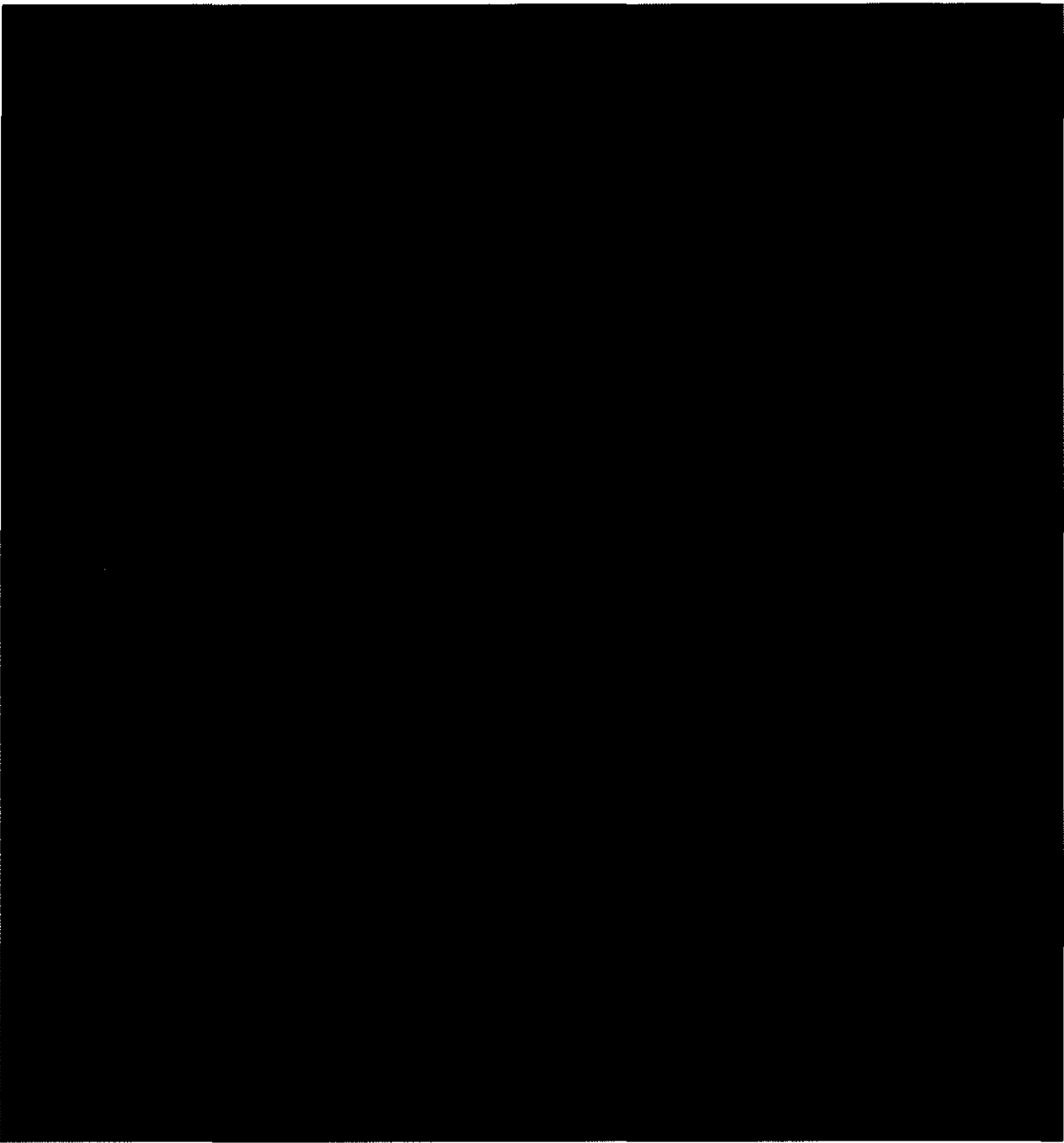
1. The President has authorized the Attorney General of the United States to approve applications for electronic surveillance for foreign intelligence information [50 U.S.C. § 1805(a)(1)];
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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

Derived from: Application to the USFISC in

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

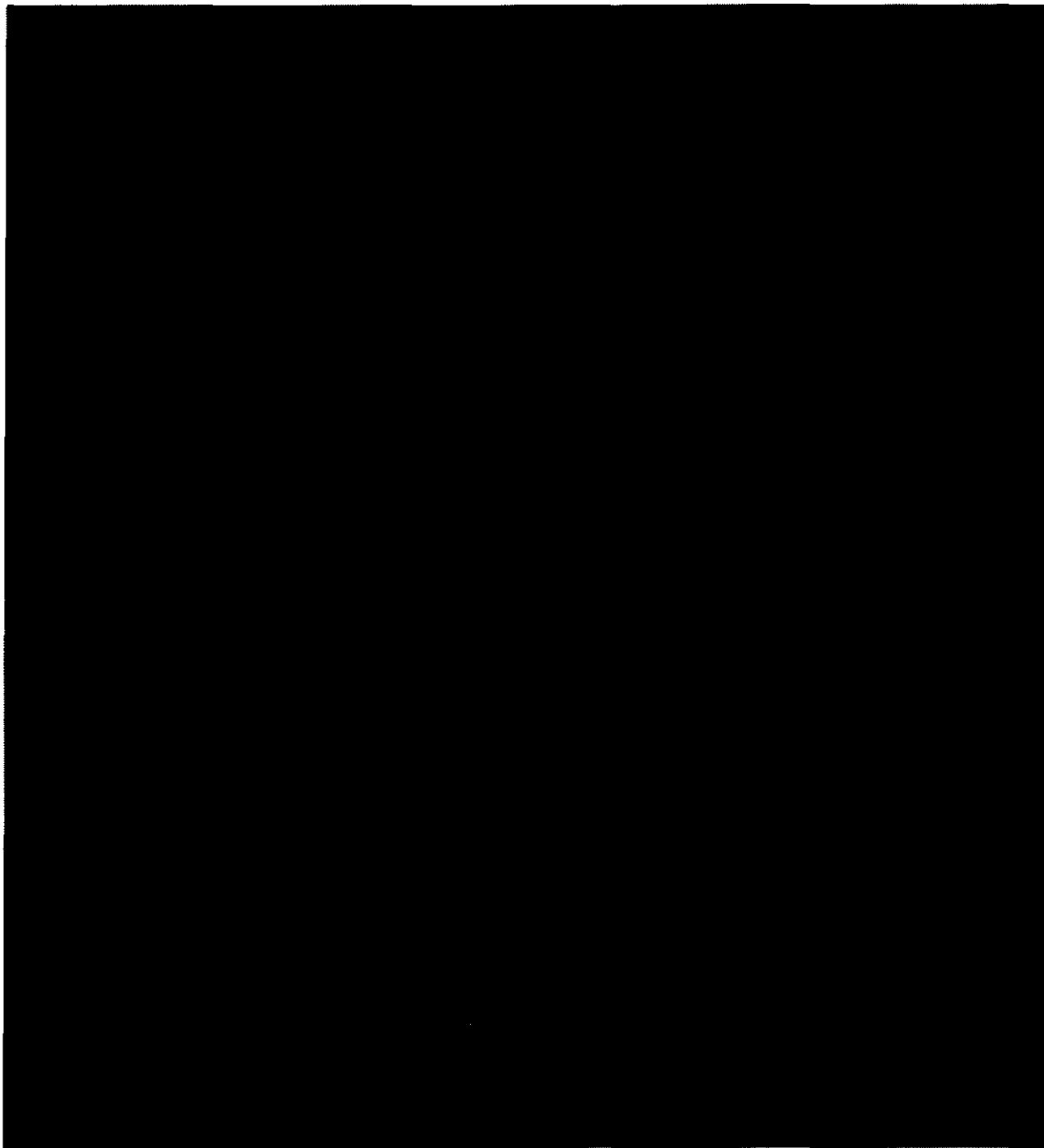
3. On the basis of the facts submitted by the applicant, there is probable cause to believe that [50 U.S.C. § 1805(a)(3)]:



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

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

APPROVED FOR PUBLIC RELEASE



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

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



1



2



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

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

(c) each of the facilities [REDACTED] at which the electronic surveillance is directed, is being used or is about to be used by these foreign powers, and electronic surveillance is authorized, using for each particular facility only such means as are identified in Exhibit A to the application for an extension [50 U.S.C. § 1805(a)(3)(B)];

4. The minimization procedures proposed in the application have been adopted by the Attorney General and, as modified herein, meet the definition of minimization procedures under 50 U.S.C. § 1801(h). [50 U.S.C. § 1805(a)(4)]; and

5. The application for an extension contains all statements and certifications required by 50 U.S.C. § 1804, and the certification is not clearly erroneous on the basis of the statements made under 50 U.S.C. § 1804(a)(7)(E), and any other information furnished under 50 U.S.C. § 1804(d). [50 U.S.C. § 1805(a)(5)].

WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States for an extension of the orders issued in the above-captioned docket number, as described in the application for an extension, is GRANTED, and it is

[REDACTED]

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

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

FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

(1) The orders issued in the above-captioned docket number, which authorized the United States to conduct electronic surveillance to acquire foreign intelligence information as defined by 50 U.S.C. § 1801(e)(1)(A) and (B), including the incidental acquisition of other foreign intelligence information as defined by 50 U.S.C. § 1801(e)(1)(C) and (2), at the facilities or places described in paragraph 3(c) above, subject to the minimization procedures specified in paragraph 4 above, including the application of the "minimization probable cause standard" specified below, are hereby extended for the period specified herein, as follows:



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

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

[REDACTED], NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA

[REDACTED]

[REDACTED]

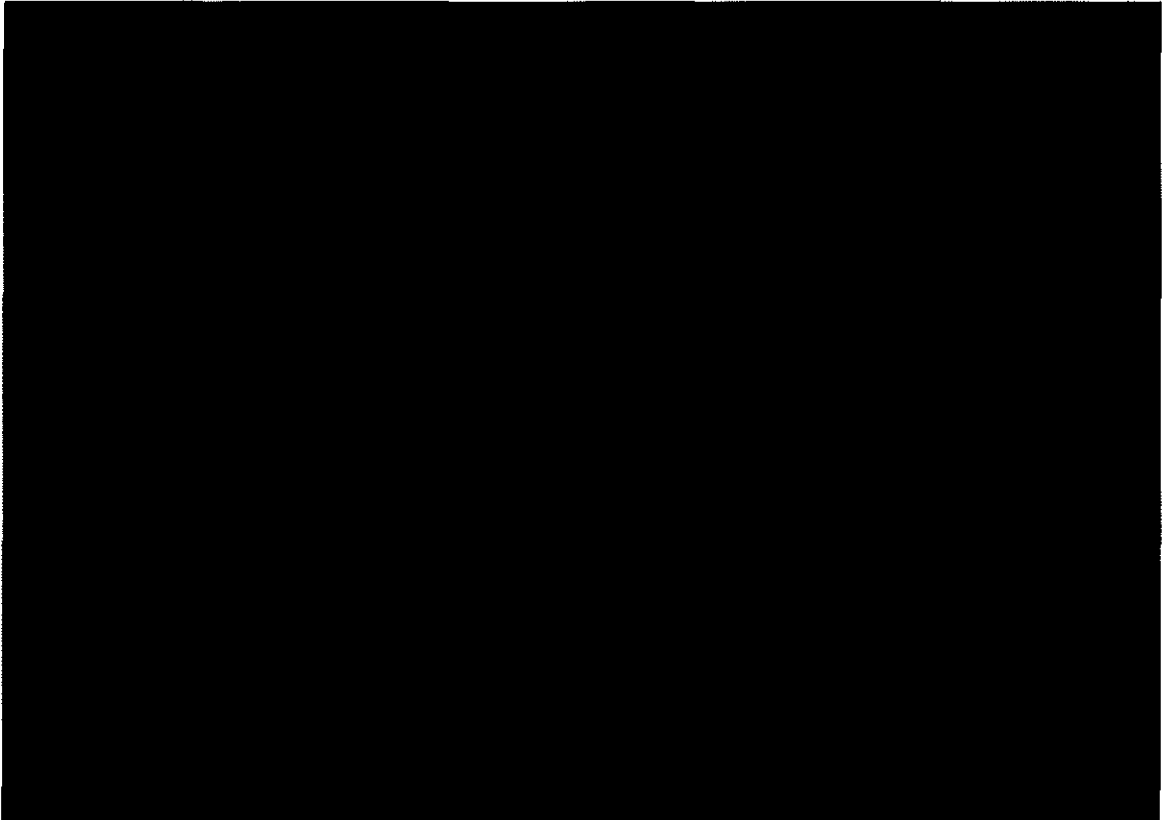
[REDACTED]

[REDACTED]

⁴ Although the NSA surveillance will be designed to acquire only international communications where one communicant is outside the United States, the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that this will be the case. In such cases, NSA shall apply its standard FISA minimization procedures, as described and modified herein, to any domestic communications it may inadvertently acquire.

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

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



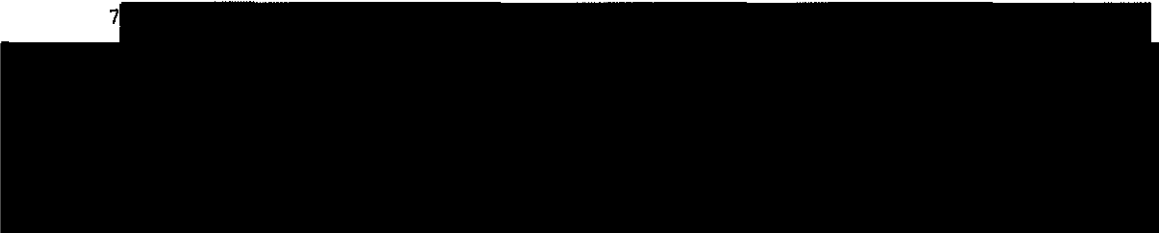
⁵ The Court understands that the system will select for delivery to NSA not only international Internet communications to and from agents or members of [REDACTED]

[REDACTED] but also Internet communications in which e-mail addresses [REDACTED] of such agents or members are mentioned in the Internet communication.

⁶



⁷

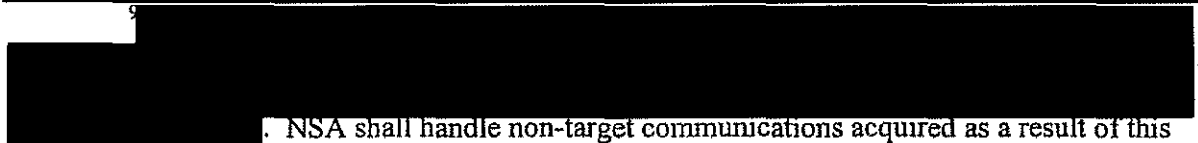
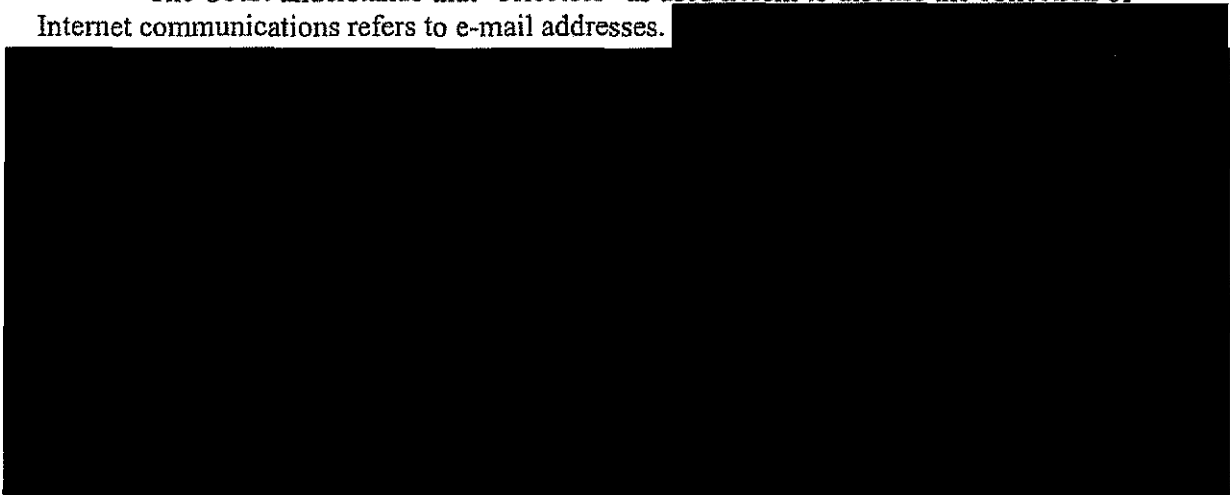


~~TOP SECRET//COMINT//NOFORN~~

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



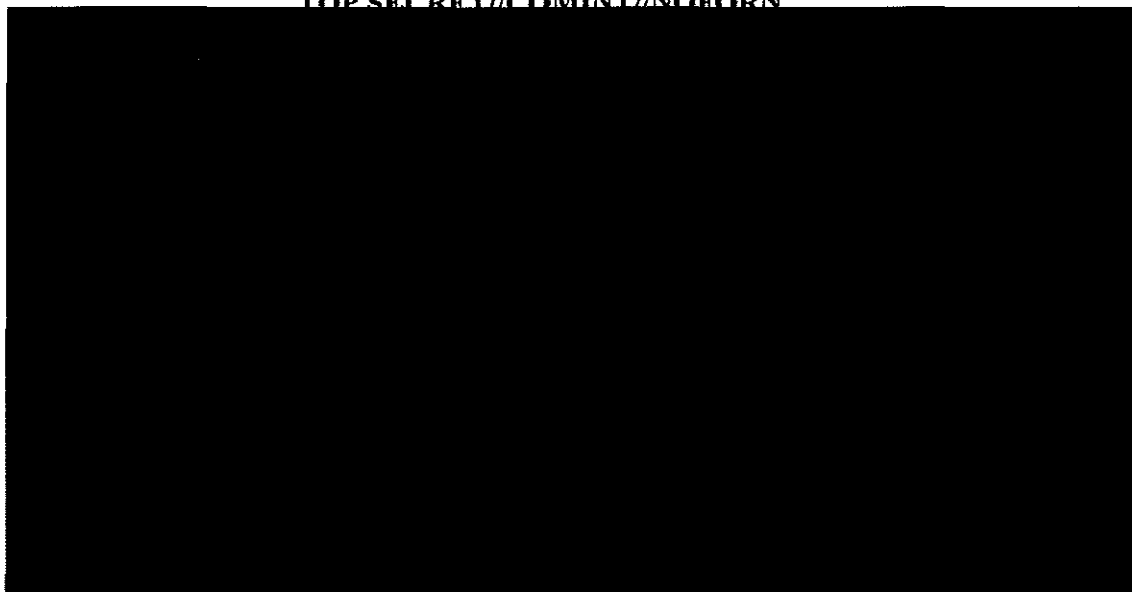
⁸ The Court understands that "selectors" as used herein to discuss the collection of Internet communications refers to e-mail addresses.



. NSA shall handle non-target communications acquired as a result of this technical limitation in accordance with its standard FISA minimization procedures, as modified herein.

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

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



Unconsented physical entry is not authorized to implement the electronic surveillance approved herein.

(2) The person(s) specified in the secondary orders attached hereto, specifically:



10



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

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

[REDACTED]

including all assigns and/or other successors in interest to said specified persons with regard to the facilities and/or places targeted herein, shall:

(a) furnish the United States all information, facilities, and/or technical assistance necessary to effect the authorities granted herein in accordance with the orders of this Court directed to said specified person; and

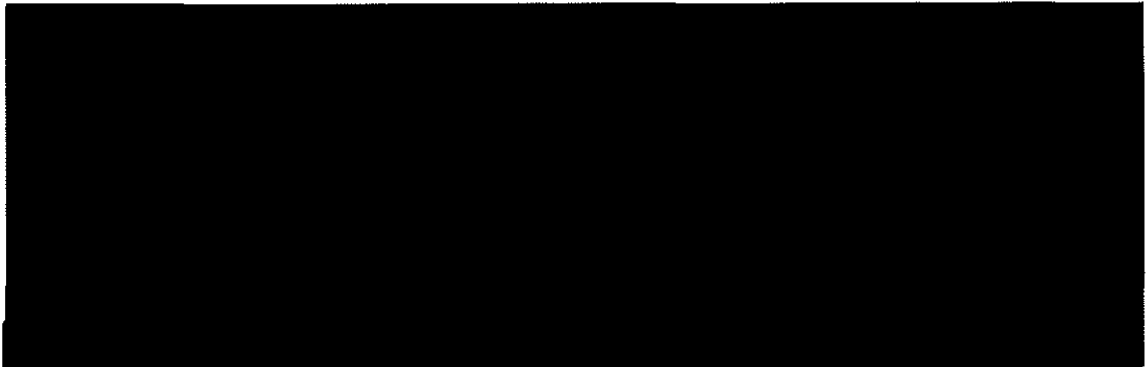
(b) maintain all records concerning this matter, or the aid furnished to the United States, under the security procedures approved by the Attorney General and the Director of Central Intelligence (or the Director of National Intelligence) that have previously been or will be furnished to the specified persons and are on file with this Court, and the United States shall compensate any such person(s) providing assistance at the prevailing rate for all assistance furnished in connection with the activities described herein [50 U.S.C. §§ 1805(c)(2)(B)-(D)].

(3) As to all information gathered through the authorities requested herein, the NSA shall follow the minimization probable cause procedure set forth below:

Minimization Probable Cause Standard. NSA shall apply two criteria in selecting communications to target for collection, both of which shall apply in each instance. First, NSA shall compile and update a list of telephone numbers and e-mail addresses (together, "selectors") for which it has determined, based on the totality of circumstances, there is probable cause to believe that the particular selector is used by [REDACTED]

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

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



Second, NSA shall acquire only communications for which there is probable cause to believe that at least one of the communicants is outside the United States. Together, these two criteria constitute the "minimization probable cause standard."

Use of Foreign Selectors. All selectors shall be telephone numbers or e-mail addresses that NSA reasonably believes are being used by persons outside the United States.¹¹

NSA Process for Determining that the Minimization Probable Cause Standard Has Been Met. All telephone numbers and e-mail addresses NSA analysts seek to use as a basis for acquiring communications from the facilities [REDACTED]

[REDACTED] shall be entered into a database that will show the telephone number or e-mail address the analyst has probable cause to believe is used by a member or agent of [REDACTED]

[REDACTED] and a statement of the

¹¹ The Court understands that a selector that NSA reasonably believes is being used outside the United States may on occasion be used in the United States. If NSA discovers that it has acquired communications from a selector while that selector was being used inside the United States, NSA shall handle any such inadvertently acquired communications as provided in the minimization procedures described in this Order.

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

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

reasons for such a belief. [REDACTED] as described in Exhibit A to the application for an extension. The proposed number or e-mail address and supporting documentation shall be reviewed by officials from the [REDACTED] Branch within NSA.¹² Prior to initiating acquisition of communications to or from a telephone number or to, from, or concerning an e-mail address [REDACTED] NSA officials from the [REDACTED] [REDACTED] Branch shall confirm that documentation regarding the first prong of the minimization probable cause standard is present in the file. If the reviewing officials find that the standard has not been documented appropriately, the telephone number or e-mail address will remain in the database, but shall be ineligible for tasking and will be designated as such.

Additional Oversight. The NSA shall apply the following additional oversight. The NSA's Inspector General (IG), General Counsel (GC), and the Signals Intelligence Directorate's Office of Oversight and Compliance shall each periodically review this electronic surveillance to ensure that it is being carried out lawfully, including that the processing and dissemination of U.S. person information is being accomplished in accordance with the procedures described herein.

¹² The Court understands that NSA is considering assigning this duty to another NSA component. If such a change in the assignment of this duty occurs and if different officials will determine whether proper documentation exists to support the determination that specific telephone numbers, e-mail addresses [REDACTED] meet the minimization probable cause standard, the Government shall inform the Court in the next application for a renewal of the Court's authorization.

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

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

Review by the Department of Justice and Reporting to this Court:

- (i) An attorney from the National Security Division at the Department of Justice shall review the NSA's justifications for targeting selectors.
- (ii) The Government shall submit a report to the Court every thirty (30) days listing new selectors that the NSA has tasked during the previous thirty days and briefly summarizing the basis for the NSA's determination that the first prong of the minimization probable cause standard has been met for each new selector.
- (iii) At any time, if the Court finds that there is not probable cause to believe that any particular selector is used by a member or agent of [REDACTED]

the

Court may direct that surveillance under this Order shall cease on that selector expeditiously. The Court may also direct that any communications acquired using that particular selector shall be segregated and/or disposed of in a manner approved by the Court.

(4) In addition to the minimization probable cause standard set forth above, as to all information gathered through the authorities requested herein, NSA shall follow:

(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

and b(7)(E)

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

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

[REDACTED]

1. The following shall be added to the end of Section 3(f) of these standard NSA

FISA procedures:

(7) The National Security Division of the Department of Justice 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.

2. The following shall be added to the end of Section 4(b) of these standard 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 the Assistant Attorney General for the National Security Division or his designee.

3. The following shall replace subsections (a), (b), and (c) of Section 8 of these standard NSA FISA procedures:

NSA may disseminate nonpublicly-available identity or personally identifiable information concerning United States persons to foreign governments provided that such information is foreign intelligence information and either (i) the Attorney General approves the dissemination; or (ii) NSA disseminates the information under procedures approved by the Attorney General. In addition, NSA may disseminate such foreign intelligence information, to the extent authorized by the Director of National Intelligence (DNI) and in accordance with DNI directives, subject to the following procedures:¹³

[REDACTED]

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

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

(1) Disseminations to [REDACTED] may be made upon the approval of any person designated for such purpose by the Director of NSA.

(2) Disseminations to [REDACTED] foreign governments may be made upon the approval of the NSA's Office of General Counsel, upon consideration of the following factors: the national security benefit the United States may reasonably expect to obtain from making the dissemination; the anticipated uses to which the foreign government will put the information; and any potential for economic injury, physical harm, or other restriction of movement to be reasonably expected from providing the information to the foreign government. If the proposed recipient(s) of the dissemination have a history of human rights abuses, that history should be considered in assessing the potential for economic injury, physical harm, or other restriction of movement, and whether the dissemination should be made. In cases where there is a reasonable basis to anticipate that the dissemination will result in economic injury, physical harm, or other restriction of movement: (i) the approval of the NSA's Signals Intelligence Director will also be required; and (ii) if dissemination is approved, NSA will undertake reasonable steps to ensure that the disseminated information will be used in manner consistent with United States law, including Executive Order No. 12,333 and applicable federal criminal statutes.

(3) NSA 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 National Security Division, United States Department of Justice, on at least an annual basis.

4. Regarding dissemination of evidence of a crime, Sections 5(a)(2) and 6(b)(8) of these standard NSA FISA procedures shall be superseded 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), 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.

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

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

5. The following shall be added to end of Section 6 of these standard NSA FISA

procedures:

NSA may disseminate all communications acquired to the CIA, which shall process any such communications in accordance with minimization procedures approved by this Court.

(c) The following additional modifications to the standard NSA FISA minimization procedures for electronic surveillance:

1. Notwithstanding sections 3(c)(2) and (e), 5(b), and 6(a) of the standard NSA FISA procedures, communications acquired under this Order may be retained for five years, unless this Court approves retention for a longer period. The communications that may be retained under this Order include electronic communications acquired because of limitations on NSA's ability to filter communications, as described in Exhibit A to the application for an extension.

2. Section 3(c)(6) of these standard NSA FISA minimization procedures is deleted and replaced with:

To the extent reasonably possible, NSA personnel with access to the data acquired pursuant to this authority shall query the data in a manner designed to minimize the review of communications of or concerning U.S. persons that do not contain foreign intelligence information or evidence of a crime.

3. Section 3(g)(1) of these standard NSA FISA minimization procedures, relating to absences "from premises under surveillance" by agents of a foreign power, shall not apply to this surveillance.

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

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

(5) The CIA shall minimize all communications received under this order as provided in Exhibit F to the initial application filed in the above-captioned docket number.

Signed 4.5.2007 1:15 pm Eastern Time
Date Time

This authorization regarding

[REDACTED]

expires at 5:00 p.m. Eastern Time

on the 31st day of May, 2007.



MALCOLM J. HOWARD

Judge, United States Foreign
Intelligence Surveillance Court

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

[REDACTED]

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

b(6) and b(7)(C)

CLERK

UNITED STATES

02

FOREIGN INTELLIGENCE SURVEILLANCE COURT

U.S. Foreign Intelligence
Surveillance Court

WASHINGTON, D.C.

IN RE

(S)

Docket Number: b(7)(E)

SUPPLEMENTAL MEMORANDUM OF LAW IN SUPPORT OF APPLICATION FOR
AUTHORITY TO CONDUCT ELECTRONIC SURVEILLANCE OF

Classified by:

b(6) and b(7)(C)

Deputy Counsel

for Intelligence Operations, NSD, DOI

Reason: 1.4(c)

Declassify on: X1

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

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

INTRODUCTION (U)

This Court requested additional briefing in the above-captioned matter, in which the United States has sought authorization to establish an early warning system under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801-1862, to alert the United States to international communications of members or agents of the [REDACTED] foreign powers:

[REDACTED]
Specifically, the Court requested an additional submission addressing whether the Application's request to [REDACTED]

[REDACTED] specifically described in the supporting documents is consistent with FISA's requirement that the application specify the "facilities or places at which the electronic surveillance is directed." 50 U.S.C. § 1804(a)(4)(B). The Court's questions concerned (i) whether [REDACTED]

[REDACTED]; and (ii) whether [REDACTED]

[REDACTED] As further explained below, the [REDACTED]

[REDACTED] as the "facilities" at which surveillance is "directed" is fully consistent with the plain and ordinary meaning of these statutory terms; with the overall structure and purpose of FISA; and with this Court's precedents.¹ ~~(TS//NF)~~

¹ The National Security Agency has reviewed this memorandum of law for factual accuracy. (U)

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

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

I. Directing Surveillance at the “Facilities” [REDACTED] Will Establish a Technologically Feasible and Effective Means for Collecting Vital Intelligence About the Targets that Would Otherwise Be Lost (S)-

One of the most serious challenges the United States confronts in its efforts to prevent another catastrophic terrorist attack on the Nation is the need quickly and effectively to track members and agents of international terrorist groups who manipulate modern technology in an attempt to communicate without detection. Declaration of John S. Redd, Director, National Counterterrorism Center ¶¶ 141-153 (Dec. 11, 2006) (Exhibit B to the Application) (“NCTC Declaration”). The [REDACTED] foreign powers that would be targeted by the proposed surveillance—[REDACTED]

[REDACTED]—pose the most serious of these threats. *Id.* ¶ 157. The Application proposes an “early warning” system under FISA aimed at addressing this national security imperative. The system would dramatically improve foreign intelligence surveillance of these target groups under FISA [REDACTED]

² (TS//NF)-

FISA authorizes the surveillance proposed in the Application. The Application satisfies FISA’s statutory requirements by:

- establishing that there is probable cause to believe that the [REDACTED] of the surveillance are foreign powers, 50 U.S.C. § 1805(a)(3)(A); NCTC Declaration ¶¶ 7-134; Memorandum of Law in Support of Application for Authority to Conduct Electronic Surveillance of [REDACTED]

² [REDACTED]

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

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

[REDACTED]
at 15-22 (Dec. 12, 2006) (Exhibit A to the Application) ("Memorandum of Law");

- demonstrating that there is probable cause to believe that each of the facilities [REDACTED] is being used or is about to be used by a foreign power or its agents, 50 U.S.C. § 1805(a)(3)(B); Declaration of Lieutenant General Keith B. Alexander, Director of the National Security Agency ¶¶ 12-18, 38, 41, 44, 48, and 51-63 (Dec. 12, 2006) (Exhibit C to the Application) ("NSA Declaration"); Memorandum of Law at 33-36; and,
- setting forth rigorous and extensive minimization procedures that meet FISA's statutory standard, 50 U.S.C. § 1805(a)(4); Application ¶ 5; Memorandum of Law at 36-52.

As will be discussed in detail below, [REDACTED]

[REDACTED] are "facilities" as that term is used in FISA, and the surveillance proposed is "directed" at those facilities. It merits emphasis at the outset, however, why the Government has proposed the method of surveillance set forth in the Application—that is, why the more typical FISA approach would be inadequate to serve the critical early warning function that is the very purpose of the surveillance proposed in the Application. (~~S//SI//NF~~)

An effective early warning system must conduct surveillance with speed and agility that cannot be obtained through the more traditional approach of filing individual applications directed at specific e-mail addresses and phone numbers. To begin with, [REDACTED]

[REDACTED]
[REDACTED] Declaration of [REDACTED], NSA Program
Manager for Counterterrorism Special Projects, National Security Agency ¶ 21 (Jan. 2, 2006)
("Supplemental NSA Declaration"). [REDACTED]
[REDACTED]

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

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

[REDACTED]

[REDACTED] NCTC Declaration ¶ 149; NSA Declaration ¶ 23; Supplemental NSA Declaration ¶¶ 15-16, 25. Were surveillance to be conducted by filing individual FISA applications for each new e-mail address and telephone number, the Court and the Government would confront a dramatic increase in emergency applications. The Government anticipates that, if the Application is approved, it will initiate collection [REDACTED] new telephone numbers and e-mail addresses each month. NSA Declaration ¶ 22; Supplemental NSA Declaration ¶¶ 19, 24. That would translate to filing a motion to amend a FISA order (or seeking Attorney General emergency authority) as many as [REDACTED] times each day, or filing one motion (or seeking one Attorney General authorization and filing a related application with the Court) covering as many as [REDACTED] new selectors each day if the surveillance were directed at specific telephone numbers and e-mail addresses. See Supplemental NSA Declaration ¶ 24. (TS//SI//NF)

But the difficulty with conducting the proposed surveillance using the more common framework of directing surveillance at specified telephone numbers and e-mail addresses to collect communications to and from them transcends the very real problem of resource constraints. Even if the Government were to seek emergency authorizations rather than filing individual applications with the Court before initiating collection on new telephone numbers and e-mail addresses, valuable intelligence *inevitably* would be lost, even given efficient processing of applications. *Id.* ¶ 25. [REDACTED]

[REDACTED] A significant advantage of allowing trained NSA analysts to make targeting decisions "on the ground" is that, once an analyst learns of a previously unknown telephone

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

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

number or e-mail address and determines that the number or address is reasonably believed to be used by a member or agent of [REDACTED] NSA generally can quickly initiate collection of communications to and from that number or address. *Id.* ¶ 22; *see also* NSA Declaration ¶ 23 (“Under established FISA procedures, NSA is unable to obtain authorization in time to immediately collect operational information sent to and from these new accounts, potentially losing vital information forever. . . . [T]he proposed collection procedures would permit NSA to rapidly analyze terrorist communications [and make it more likely for the NSA] to uncover quickly the existence of previously unknown terrorists.”). (TS//SI//NF)

The collection of communications transmitted between the time that an NSA analyst could task an account and the time that the Attorney General would have been able to grant emergency authorization under section 105(f) of FISA is critical to the operation of the early warning system—it is always advantageous to collect intelligence as quickly as possible, and in some cases that information otherwise would be lost forever. *See* Supplemental NSA Declaration ¶¶ 23-25; NCTC Declaration ¶ 152 ([REDACTED])

[REDACTED] d. In short, the proposed surveillance would enable collection of critical intelligence because the Government could target new telephone numbers and e-mail addresses with a higher degree of speed and agility than would be possible through the filing of individual FISA applications or requests for emergency approval. Supplemental NSA Declaration ¶¶ 23-24. (TS//SI//NF)

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

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

And there are other ways in which the proposed surveillance would enable collection of communications that otherwise might not be acquired. Using the framework proposed in the Government's Application, rather than the more customary framework of directing surveillance at specified telephone numbers and e-mail addresses and collecting only communications to and from them, would allow the discovery and interception of new information about terrorist suspects. Supplemental NSA Declaration ¶ 27. [REDACTED]

[REDACTED] Obtaining these communications is essential to achieving the objectives of the proposed Order. ~~(TS//SI//NF)~~

[REDACTED] the NSA can collect communications not only to and from a tasked e-mail address, but also communications in which a tasked e-mail address appears in the substantive contents of a communication between two third parties. Supplemental NSA Declaration ¶ 28. (For example, [REDACTED]

[REDACTED] *Id.* ¶ 28.) [REDACTED]

[REDACTED] *Id.* ¶ 27. [REDACTED]

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

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



For all the reasons described above, by [REDACTED]

[REDACTED] the Government's

proposed surveillance would collect vital intelligence information that otherwise would be lost, and thereby invaluablely contributes to the proposed early warning system under FISA. ~~(S//SI//NF)~~

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

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

II. The "Early Warning" System Set Forth in the Application is Fully Consistent With FISA (S)

A. FISA Establishes a Flexible and Common-Sense Regime for the Conduct of Foreign Intelligence Surveillance (U)

When it enacted FISA in 1978, Congress recognized the need for flexibility in the field of foreign intelligence collection. *See* H.R. Rep. No. 95-1283, Pt. I, at 27 (1978) ("No means of collection are barred by the bill, and the circumstances justifying collection are fully responsive to the intelligence agencies' needs as they have been expressed to this committee."); *see also id.* at 38 (1978) (explaining that the term "clandestine intelligence gathering activities" used in FISA "is supposed to be flexible with respect to what is being gathered because the intelligence priorities and requirements differ between nations over time, and this bill is intended to allow surveillance of different foreign powers' intelligence activities well into the future"). Congress prudently recognized that different methods of conducting electronic surveillance may be necessary to address different foreign intelligence threats. Accordingly, FISA places few specific constraints [REDACTED]

[REDACTED] at which surveillance may be directed. Nor does FISA reflect (as does its criminal analogue, Title III, 18 U.S.C. §§ 2510-2522) a statutory directive regarding the particular manner in which the information collected through electronic surveillance must be minimized.⁴ Instead, the central findings that the Court must make in exercising jurisdiction over the proposed electronic surveillance are straightforward and few: that there is probable cause to believe that the target is a foreign power or an agent of a foreign power, *see* 50 U.S.C.

⁴ *See* 18 U.S.C. § 2518(5) (requiring that interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under" Title III). FISA's legislative history confirms that FISA was not intended to have Title III's more stringent requirements for minimization at the point of acquisition. *See* H.R. Rep. 95-1293, pt. I, at 56 (1978) ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be as strict as under [Title III]."). (U)

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

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

§ 1805(a)(3)(A); that there is probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power," *id.* § 1805(a)(3)(B); and that the "proposed minimization procedures meet the definition of minimization procedures" under FISA, *id.* § 1805(a)(4). The term "minimization procedures," in turn, is defined fundamentally by reference to the surveillance's reasonableness; these procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of certain U.S. person information "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1801(h)(1). (S)

When considered together, these requirements establish a flexible, common-sense regime that allows the Government to propose, and the Court to approve, a wide range of methods for conducting foreign intelligence surveillance. This flexibility allows FISA to serve as a powerful tool for foreign intelligence collection while at the same time protecting the privacy of United States persons. FISA accomplishes these two objectives by placing few constraints on the manner in which surveillance is conducted, but at the same time requiring court-approved minimization procedures that are reasonable in light of the overall purpose and technique of the surveillance. *See* 50 U.S.C. § 1801(h); *see also* H.R. Rep. No. 95-1283, Pt. I, at 55 (1978) ("It is recognized that minimization procedures may have to differ depending upon the technique of the surveillance."). If the nature of the target (including the target's tradecraft) or the technology involved renders it advantageous to define the facilities broadly, FISA does not preclude the surveillance; instead, it allows the Government to conduct the surveillance if the Government

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

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

adopts rigorous minimization procedures, approved by this Court, that ensure that the privacy interests of U.S. persons are properly protected. *See, e.g.*, H.R. Rep. No. 95-1283, Pt. I, at 55 (1978) (“[I]n many cases it may not be possible for technical reasons to avoid acquiring all information. In those situations, the reasonable design of procedures must emphasize the minimization of retention and dissemination.”). (S)

As will be explained in detail below, this Court’s practice and precedents reflect the flexibility inherent in FISA’s statutory scheme. This Court has frequently authorized the Government to conduct surveillance in unique ways in response to changing technologies or difficult foreign intelligence challenges, after assuring itself that the surveillance would be conducted in a manner that reasonably protected the privacy interests of U.S. persons.⁵ *See infra* § II.B.2. Viewed in this light, the Court’s approval of this unique Application—under which surveillance would be [REDACTED] but would be conducted pursuant to extensive and rigorous minimization procedures—would be fully consistent with the text of FISA, its broader purpose, and this Court’s precedents. (TS//NF)

B. [REDACTED] Constitute “Facilities” Under FISA (TS)

This Court has specifically inquired about whether the term “facilities” in FISA limits the Government to directing surveillance at individual e-mail addresses and telephone numbers [REDACTED]

⁵ In emphasizing the flexibility that inheres in FISA, the Government is not suggesting that FISA requires this Court to approve surveillance once it finds that a particular application proposes surveillance that would be “directed” at “facilities” as those terms are used in FISA. This Court retains considerable discretion to determine that proposed minimization procedures meet the definition of minimization procedures under FISA, and to determine whether the surveillance meets the requirements of the Fourth Amendment. (U)

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

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

[REDACTED]

[REDACTED] would be consistent with FISA's statutory scheme, which allows the Government the flexibility to optimize surveillance against national security threats, subject to reasonable minimization procedures, in order to achieve the objectives of the particular surveillance. *See supra* § II.A. As shown below, this understanding of the word "facilities" also is consistent with the plain meaning of the term and with this Court's precedents. (TS//NF)

1. [REDACTED]

[REDACTED]

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

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

2, [REDACTED]

The breadth and flexibility of the term “facilities” in FISA are confirmed by this Court’s precedents. As set forth in detail in the Government’s memorandum of law, Memorandum of Law at 26-31, this Court has on numerous occasions authorized surveillance under applications that identified the “facility” [REDACTED]

[REDACTED] Most notably, in [REDACTED] Opinion and Order, No. PR/TI [REDACTED] (July 14, 2004) ([REDACTED]), this Court accepted the Government’s submission that [REDACTED] were “facilities” within the meaning of Title IV of FISA, explaining that the statute’s plain language did not “restrict the use of trap and trace devices to communications facilities associated with individual users.” *Id.* at 23.⁶ ~~(TS//NF)~~

This Court has also frequently approved applications for electronic surveillance directed at “facilities” other than individual e-mail accounts or telephone numbers. For example, in [REDACTED] and b(7)(A) [REDACTED]

6 [REDACTED]

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

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

and b(6), b(7)(A), (C), and (E)



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

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

and b(6), b(7)(A), (C), and (E)



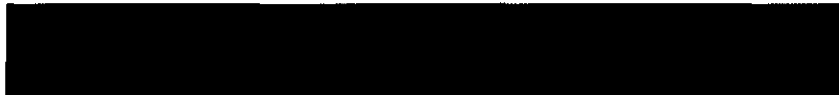
~~TOP SECRET//COMINT//NOFORN~~

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

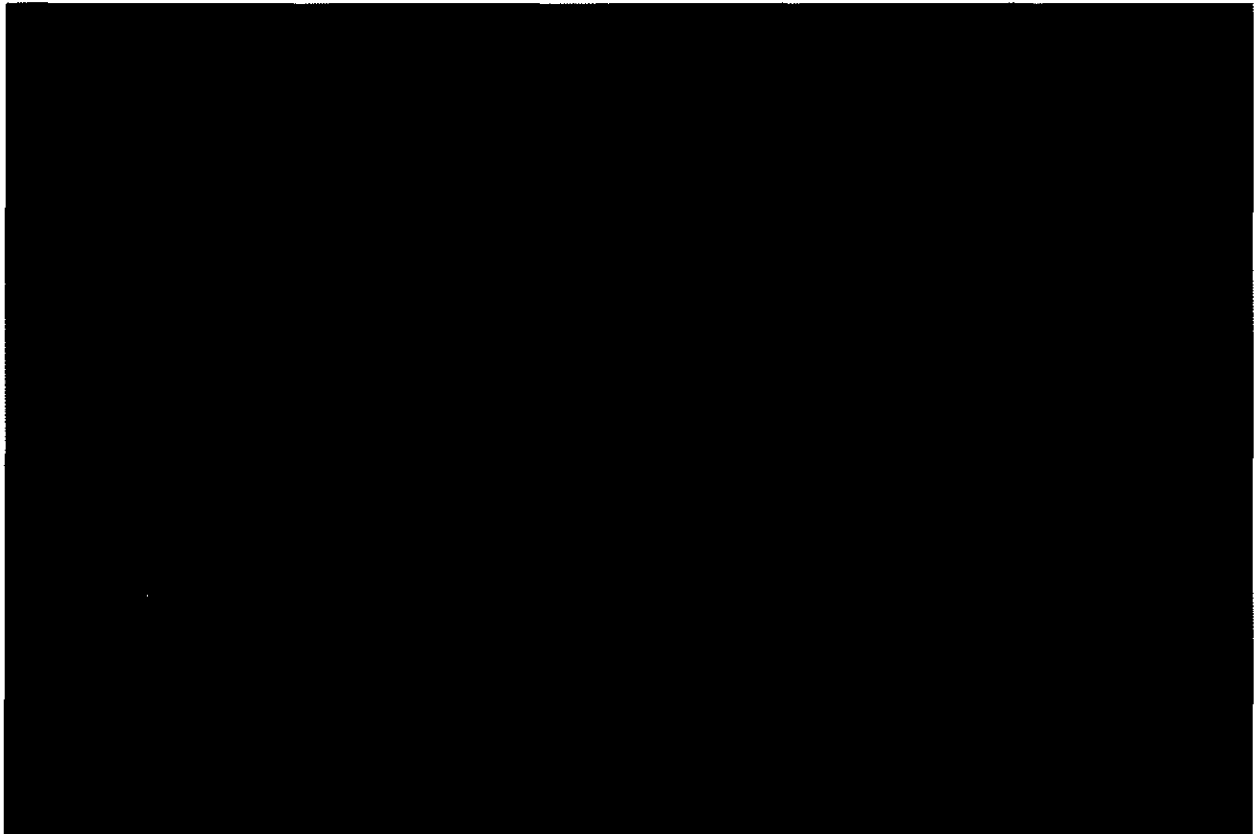
and b(7)(E)



3.



(S)



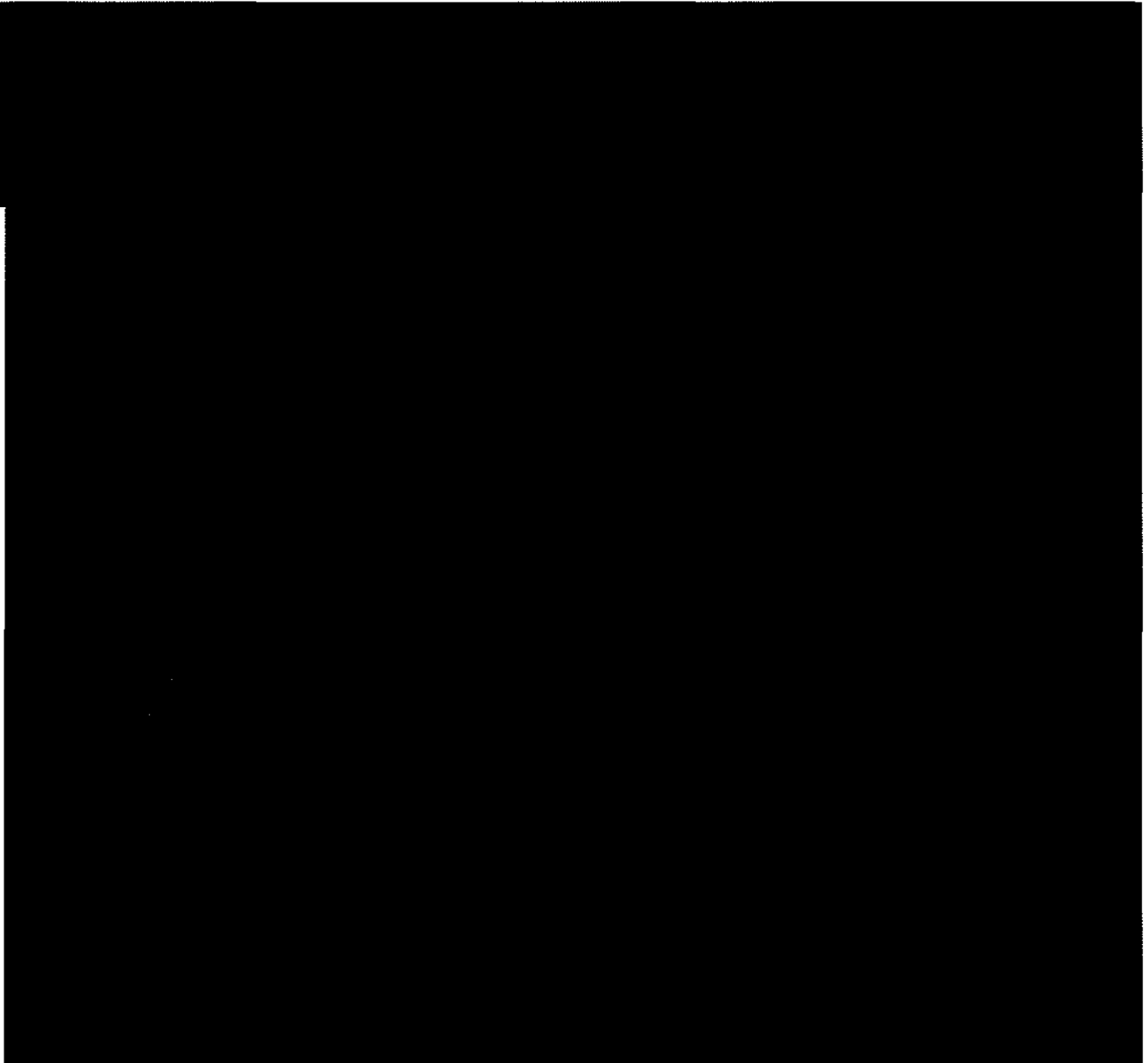
~~(TS//NF)~~

8



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

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



C. The Surveillance Proposed in the Application Would Be “Directed” at the Facilities [REDACTED] (U)

This Court has also asked whether the surveillance proposed is properly understood to be “directed” at the facilities [REDACTED]; the suggestion, as the Government understands it, is that the surveillance might be better understood as “directed” instead at the e-mail addresses and numbers the Government would task for collection under the proposed Order.

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

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

This question relates closely to the “facilities” question addressed above, and accordingly many of the arguments previously discussed—such as the flexibility that inheres in FISA’s statutory scheme, *supra* § II.A, [REDACTED]

[REDACTED] *supra* § II.B—also support the Government’s position. In the interests of completeness, however, this section explains why FISA clearly permits surveillance to be “directed” at the facilities [REDACTED]

[REDACTED] (TS) [REDACTED]

1. *The Plain Language of FISA Permits Surveillance to Be* [REDACTED]

[REDACTED] (S) [REDACTED]

FISA requires the applicant to set forth facts showing that “each of the facilities or places at which the electronic surveillance is *directed* is being used, or is about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1804(a)(4)(B) (emphasis added); *see also id.* § 1805(a)(3)(B), § 1805(c)(1)(B). Because FISA does not define the term “directed,” we look to its ordinary meaning. *See, e.g., Engine Mfrs. Ass’n v. South Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252 (2004) (“Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose.”) (quotations and citations omitted). The ordinary understanding of the term “directed” is that it refers to the places or facilities at which the Government intends to direct, or point, the surveillance device; that is, where the communications will be intercepted or the information acquired. *See Funk & Wagnalls New Standard Dictionary of the English Language* 718 (1946) (defining “direct” as “[t]o determine the direction of; especially, to cause to point or to go straight toward a thing”); *see also IV The Oxford English Dictionary* 701 (2d ed. 1989)

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

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

(defining "direct" as "[t]o cause (a thing or person) to move or point straight to or towards a place"). [REDACTED]

[REDACTED] (TS//NF)

This understanding is supported by the language of the relevant provisions, which refers to the facilities and *places* at which surveillance may be "directed." 50 U.S.C. § 1804(a)(4)(B); *see also id.* § 1805(a)(3)(B), § 1805(c)(1)(B). [REDACTED]

[REDACTED] Of course, the word "directed" should be understood to have the same meaning when it is read with respect to "facilities" as it does when it is read in conjunction with the term "places." *Cf. Brown v. Gardner*, 513 U.S. 115, 118 (1994) (The presumption that a term has the same meaning throughout a statute is "most vigorous when [the term] is repeated within a given sentence."). (S)

The conclusion that the surveillance at issue will be "directed" at the facilities [REDACTED] is confirmed by the relevant language of Title III's criminal wiretap provisions, on which this specific part of FISA, section 104(a)(4)(B), was based. *See* H.R. Rep. No. 95-1283, Pt. I, at 75 (1978) (section 104(a)(4)(B) of FISA "parallels existing law on surveillances

⁹ For example, as explained in the Memorandum of Law at 32-33. [REDACTED]

[REDACTED] (TS//SI//NF)

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

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

for law enforcement purposes"); *see also West Virginia Univ. Hosps., Inc. v. Casey*, 499 U.S. 83, 100 (1991) (citation omitted) ("[W]e construe [statutory terms] to contain that permissible meaning which fits most logically and comfortably into the body of both previously and subsequently enacted law."). Title III requires applications to contain "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii). To the extent there is any doubt, Title III's parallel provisions confirm the common-sense interpretation of "the facilities . . . at which the electronic surveillance is directed" described above: [REDACTED]

[REDACTED] (S)-

2. [REDACTED]

[REDACTED] FISA requires the Government's application to include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(B). [REDACTED]

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

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

[REDACTED]
[REDACTED] (S)

[REDACTED]
[REDACTED]
[REDACTED] The Court's order must specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." *Id.*

§ 1805(c)(1)(B). The phrase "if known" means that the order does not have to specify the nature and location of each of the facilities at the time the order is issued if that is not possible. *See* H.R. Conf. Rep. No. 107-328, at 24 (2001) (addition of phrase "if known" to section 1805(c)(1)(B) "is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance"). [REDACTED]

[REDACTED]
[REDACTED] Here, the nature and location of the facilities at which surveillance will be directed is known and has been described in detail, *see* NSA Declaration ¶¶ 37, 40, 43, 46, 51-63, and can easily be specified by the Court in its order.

(S//SI)

and b(7)(A) and (E)
[REDACTED]

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

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

and b(6), b(7)(C) and (E)

In any event, here the Government cannot identify at the time of the Application all of the telephone numbers and e-mail addresses that would be tasked for collection under the proposed Order.¹⁰ The whole objective of the proposed surveillance is to establish an early warning system that would enable the Government to uncover currently unknown telephone numbers and e-mail addresses used by members and agents of the [REDACTED] foreign powers to communicate into and out of the United States, and quickly to collect the communications to and from those numbers and addresses without missing vitally important communications—the acquisition of which could mean the difference in our efforts to thwart the next catastrophic terrorist attack on the United States.¹¹ Moreover, as explained above, see *supra* at 6-7, there are several categories of e-mail communications—such as communications that include a reference to a tasked e-mail address—that in fact are *not* captured through the traditional approach of intercepting only communications to and from a particular tasked address. [REDACTED]

¹⁰ Although the NSA will within the first authorization period provide the Court with a list of [REDACTED] foreign numbers and addresses from which it would like initially to collect communications, even that list will be subject to change as intelligence priorities shift and new information is uncovered. Supplemental NSA Declaration ¶ 19. (TS//SI//NF)

¹¹ The specific telephone numbers and e-mail addresses to be targeted will be identified by NSA analysts during the course of the proposed surveillance, and will be approved by the Court. Application ¶ 5. (TS//SI//NF)

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

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

[REDACTED]

[REDACTED]

(S//SI)

3.

[REDACTED]

(S)

[REDACTED]

See 50 U.S.C. § 1801(h)(1) (minimization procedures are “specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the *acquisition* and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information”) (emphasis added); [REDACTED] and b(7)(A)

[REDACTED]

see also H.R. Rep. No. 95-1283, Pt. I, at 55-56 (1978) (“By minimizing acquisition, the committee envisions, for example, that . . . where a switchboard line is tapped

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

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

but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party.”). (TS)

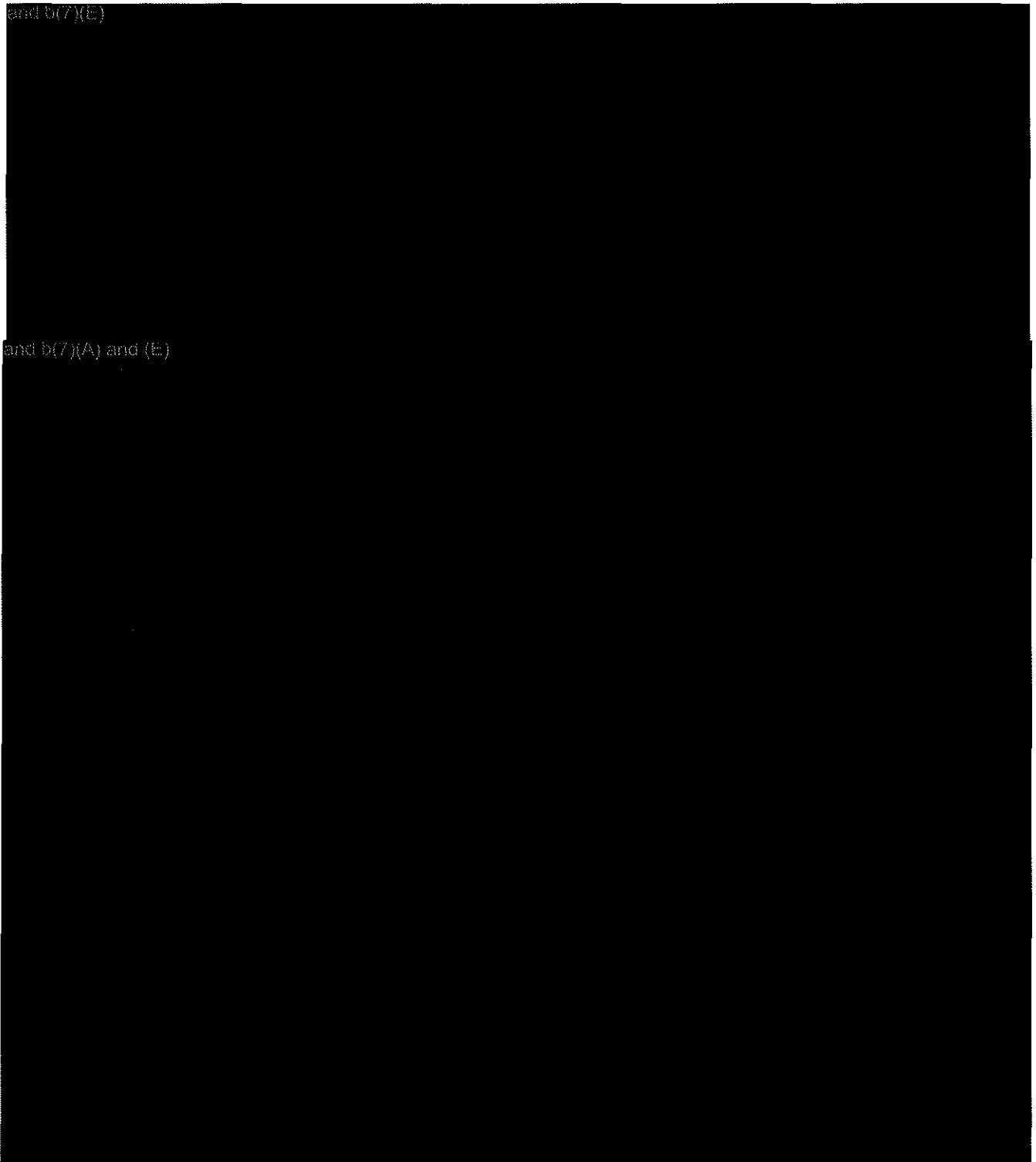
and b(6), b(7)(A), (C), and (E)



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

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

and b(7)(E)



and b(7)(A) and (E)

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

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

4.

[REDACTED]

~~(S)~~

and b(6), b(7)(A), (C), and (E)

[REDACTED]

and b(6), b(7)(A), (C), and (E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] the more typical FISA approach of filing separate FISA applications directed at specific telephone numbers and e-mail addresses would be inadequate to serve the objective of the surveillance—to establish an effective “early warning” system under FISA to detect and

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

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

prevent a catastrophic terrorist attack. *Supra* § I. [redacted] and b(6), b(7)(A), (C), and (E)

[redacted] (S)

[redacted] and b(7)(A) and (E)

[redacted] the proposed surveillance will target for collection only international communications of individuals the Government has probable cause to believe are members or agents of the [redacted] foreign powers.¹² Memorandum of Law at 36-41.

[redacted] (S)

[redacted] and b(7)(A) and (E)

[redacted] In this case, the Government confronts a unique and formidable foreign intelligence challenge—the threat posed by shadowy and nebulous terror networks that exploit modern telecommunications technology in an effort to

¹² As noted in the Government's initial Memorandum of Law, [redacted] and b(6), b(7)(C) and (E)

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

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

communicate without detection—and seeks to meet it by directing surveillance [REDACTED]

[REDACTED] subject to exacting minimization procedures. [REDACTED]

and b(7)(A) and (E)

[REDACTED] (S)

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

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

CONCLUSION (U)

For the foregoing reasons and the reasons set forth in the Government's initial Memorandum of Law, the Court should grant the requested Order. (U)

Respectfully submitted,

Dated: January 2, 2007

ALBERTO R. GONZALES
Attorney General

STEVEN G. BRADBURY
*Acting Assistant Attorney General,
Office of Legal Counsel*

JOHN A. EISENBERG
*Deputy Assistant Attorney General,
Office of Legal Counsel*

KENNETH L. WAINSTEIN
*Assistant Attorney General,
National Security Division*

MATTHEW G. OLSEN
*Acting Deputy Assistant Attorney General,
National Security Division*

BRETT C. GERRY
*Deputy Assistant Attorney General,
National Security Division*

b(6) and b(7)(C)

*Senior Counsel,
Office of Legal Counsel*

U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

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