



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*86 Chambers Street
New York, New York 10007*

December 12, 2014

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: mccrad@nytimes.com
jeremy.kutner@nytimes.com

Re: *The New York Times Co. v. U.S. Department of Justice*, 14 Civ. 3948 (VSB)

Dear David and Jeremy:

This Office represents the United States Department of Justice ("DOJ"), the defendant in the above-referenced matter. In accordance with the schedule set forth in the parties' joint submission on October 9, 2014, *see* Dkt. No. 11, as modified by the Court's December 8, 2014, order, *see* Dkt. No. 13, DOJ is releasing the enclosed documents in partial response to the Freedom of Information Act ("FOIA") request that is the subject of this litigation. These documents are responsive to categories 3 through 6 of the request. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), (b)(6), (b)(7)(A), (b)(7)(C), and (b)(7)(E). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

These documents also are being made available to the public on the Director of National Intelligence's website, "IC on the Record," at <http://icontherecord.tumblr.com/>, as well as at www.dni.gov.

If you have any questions, please do not hesitate to contact us.

Sincerely,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ Andrew E. Krause
JOHN D. CLOPPER
EMILY E. DAUGHTRY
ANDREW E. KRAUSE
Assistant United States Attorneys
Telephone: (212) 637-2716/2777/2769
Facsimile: (212) 637-0033
E-mail: john.clopper@usdoj.gov
emily.daughtry@usdoj.gov
andrew.krause@usdoj.gov

Enclosures

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

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

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2005 DEC 13 AM 11:04

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

CLERK

IN RE

Docket Number:

b(7)(E)

(S)

EXHIBIT A

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

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

Derived from Application of the United States to the Foreign
Intelligence Surveillance Court in the above-captioned
matter.

Declassify only upon the determination of the President.

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

INTRODUCTION

As the attacks of September 11th, 2001, vividly demonstrated, the United States is not immune from catastrophic terrorist attack on our own soil. Although the United States has not suffered another such attack in the five years since that day, the threat has in many ways increased. [REDACTED]

[REDACTED] Indeed, the Intelligence Community assesses that these [REDACTED] foreign powers— [REDACTED]

[REDACTED]—pose the greatest terrorist threats to the United States. [REDACTED] seek to use our own communications infrastructure and laws against us, as they secrete agents into the United States, waiting to attack at a time of their choosing. Correspondingly, one of the greatest challenges the United States confronts in the ongoing effort to prevent a subsequent catastrophic terrorist attack against the homeland is the critical need to follow up quickly on new leads. Time is of the essence in preventing terrorist attacks against our Nation. In addition, we face significant obstacles in finding and tracking members and agents of international terrorist organizations, [REDACTED] as they manipulate modern technology in an attempt to communicate while remaining undetected. Members and agents of international terrorist organizations do not wear uniforms, but instead attempt to blend into our civilian society. Speed and flexibility are essential in tracking individuals who [REDACTED]

To follow

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

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

the trails effectively, and to respond to new leads, it is vital for the U.S. Intelligence Community to be able quickly and efficiently to acquire communications to or from individuals reasonably believed to be members or agents of these [REDACTED] foreign powers.

The attached Application is intended to address these problems by establishing an early warning system under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801-1862, to alert the U.S. Government to the presence of members and agents of these foreign powers and to aid in tracking such individuals within the United States. Specifically, the Government seeks authorization from this Court to conduct electronic surveillance to collect the substantive contents of certain telephonic and electronic communications [REDACTED] foreign powers:

[REDACTED]

[REDACTED] Electronic surveillance would be conducted only at facilities for which there is probable cause to believe that the facilities are being used, or are about to be used, by those [REDACTED] foreign powers.¹

The Application is fully consistent with title I of FISA and follows in the footsteps of this Court's ground breaking and innovative decision in [REDACTED] [REDACTED] Opinion and Order, No. PR/TT [REDACTED] (July 14, 2004) ("[REDACTED]"). The Application establishes that there is probable cause to believe that the targets of the surveillance—[REDACTED]—are foreign powers under FISA. In addition, the Application demonstrates that there is probable cause to believe that [REDACTED]

[REDACTED]

¹ The National Security Agency has reviewed this memorandum of law for accuracy.

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

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

[REDACTED]—is being used or is about to be used by each of the targets. Moreover, because of the minimization procedures that will be carefully applied at the acquisition stage, collection will be targeted at only communications to or from certain telephone numbers and e-mail addresses,² i.e., those for which there is probable cause to believe: (1) that one of the communicants is a member or agent of one of the targeted foreign powers³ and (2) that the communication is to or from a foreign country.⁴ The Government would apply several additional mechanisms to ensure appropriate oversight over the collection of communications.

For example, if the telephone number or e-mail address selected for collection is reasonably believed to be used by a person in the United States, six specific procedures would be followed. (At this time, for operational reasons, it is not anticipated that the NSA will task for collection any e-mail addresses reasonably believed to be used by a person in the United States.)

- First, only three senior National Security Agency ("NSA") officials would be authorized by the Director of the NSA to approve tasking the number or address for collection—the Signals Intelligence Directorate Program Manager for Special Counterterrorism Projects, the Counterterrorism Global Capabilities Manager, and the Counterterrorism Primary Production Center Manager.

² In this memorandum, we use the term "e-mail address" [REDACTED]

We use the term "e-mail" to apply to [REDACTED]

³ In addition to collecting communications to or from an e-mail address associated with the targets, the Government would collect communications specifically referring to that particular e-mail address in the body of the message. For example, there is certainly probable cause to believe that at least one party to a communication that mentions an e-mail address used by [REDACTED]

[REDACTED] For ease of discussion, any reference in this memorandum to communications "to or from" an e-mail address for which there is probable cause to believe that the address is used by a member or agent of one of the targets includes communications referring to that e-mail address.

⁴ For ease of reference, this standard will be referred to as the "minimization probable cause standard."

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

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

- Second, all such authorizations would be documented in writing and supported by a written justification explaining why the selected telephone numbers or e-mail addresses meet the minimization probable cause standard.
- Third, the number or e-mail address may not be tasked for collection without the prior approval of the Attorney General, the Assistant Attorney General for the National Security Division (AAG/NSD), or the Deputy Assistant Attorney General in the National Security Division with responsibility for FISA operations and oversight (DAAG).
- Fourth, no such telephone number or e-mail address may be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.
- Fifth, tasking such phone numbers and e-mail addresses for collection must be explicitly approved by this Court.
 - The Government would report to the Court twice a week on any new numbers or addresses that are reasonably believed to be used by persons in the United States. Included within each report will be a description of the basis for the determination by the NSA and the Attorney General, the AAG/NSD, or the DAAG that there was probable cause to believe that the number or address is associated with a member or agent of [REDACTED]
 - If the Court does not approve any of the new telephone numbers or e-mail addresses within forty-eight hours of receiving the report because the Court does not agree that there is probable cause to believe that the number or address is associated with a member or agent of [REDACTED] the Government would have twenty-four hours to submit additional information.
 - If the Court does not, within twenty-four hours of receiving additional information from the Government, find that there is probable cause to believe that any of the new telephone numbers or e-mail addresses is associated with a member or agent [REDACTED] the tasking of that number or address must cease and any acquired communications must be segregated and may be retained only upon Court approval if the Government demonstrates a foreign intelligence need for such retention.
- Finally, the NSA would institute a system that ensures that telephone numbers and e-mail addresses of persons reasonably believed to be in the United States would be reviewed every 90 days to determine whether the collection of communications to or from the number or address should continue.

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

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

See Declaration of Lieut. Gen. Keith B. Alexander, U.S. Army, Director, National Security Agency ¶ 68 (Dec. 12, 2006) (Exhibit C to the Application) ("NSA Declaration").

Telephone numbers and e-mail addresses not reasonably believed to be used by a person in the United States would be tasked only after an NSA analyst has documented in writing his determination that the number or address meets the minimization probable cause standard and an official in the NSA's [REDACTED] Branch has verified that the analyst's determination has been properly documented. *Id.* ¶ 67. In addition, an attorney from the National Security Division at the Department of Justice would review the NSA's justifications for targeting these numbers and addresses. Every thirty days, the Government would submit a report to the Court listing new numbers and addresses that are not reasonably believed to be used by persons in the United States and that the NSA has tasked during the previous thirty days and briefly summarizing the basis for NSA's determination that there was probable cause to believe that each number and address is used by a member or agent of [REDACTED]

[REDACTED] At any time, the Court may request additional information on particular numbers or addresses and, if the Court finds that the minimization probable cause standard has not been met, the Court may direct that collection shall cease within forty-eight hours on that number or address. The Court may also direct that any communications acquired using those particular numbers or addresses must be segregated and may be retained only upon Court approval if the Government demonstrates a foreign intelligence need for such retention.

Finally, as we explain below, taking into account the nature of the national security threat posed by the targeted groups and the totality of the circumstances surrounding the proposed

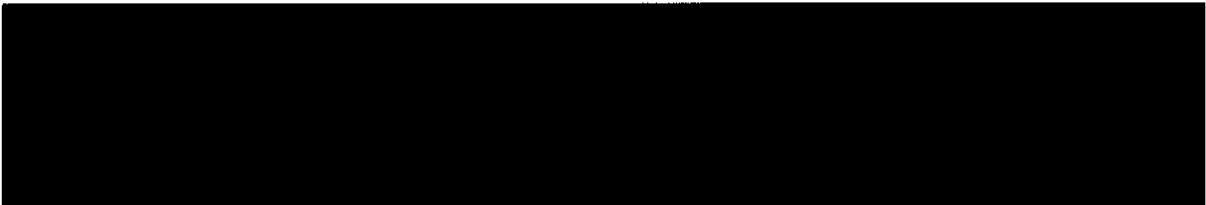
~~TOP SECRET//HUMINT//COMINT//NOFORN~~

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

surveillance, the surveillance detailed in the Application is reasonable under the Fourth Amendment.⁵

BACKGROUND

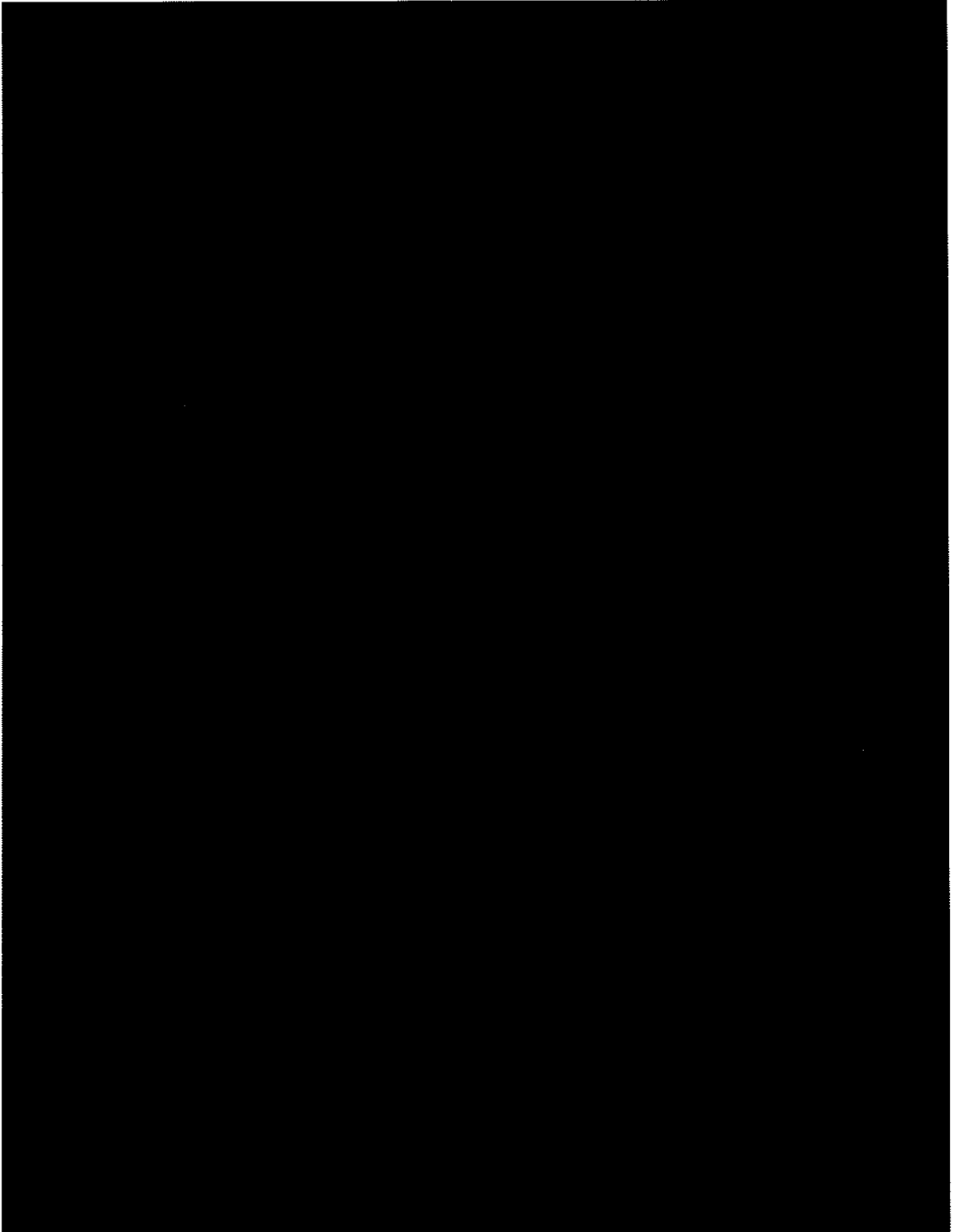
On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a direct blow at the leadership of the Government of the United States. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. These attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.



⁵ By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization.

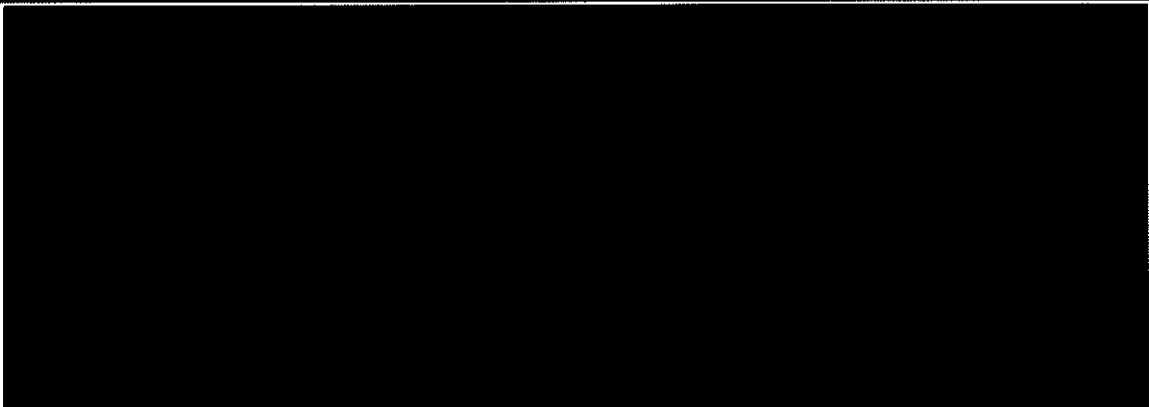
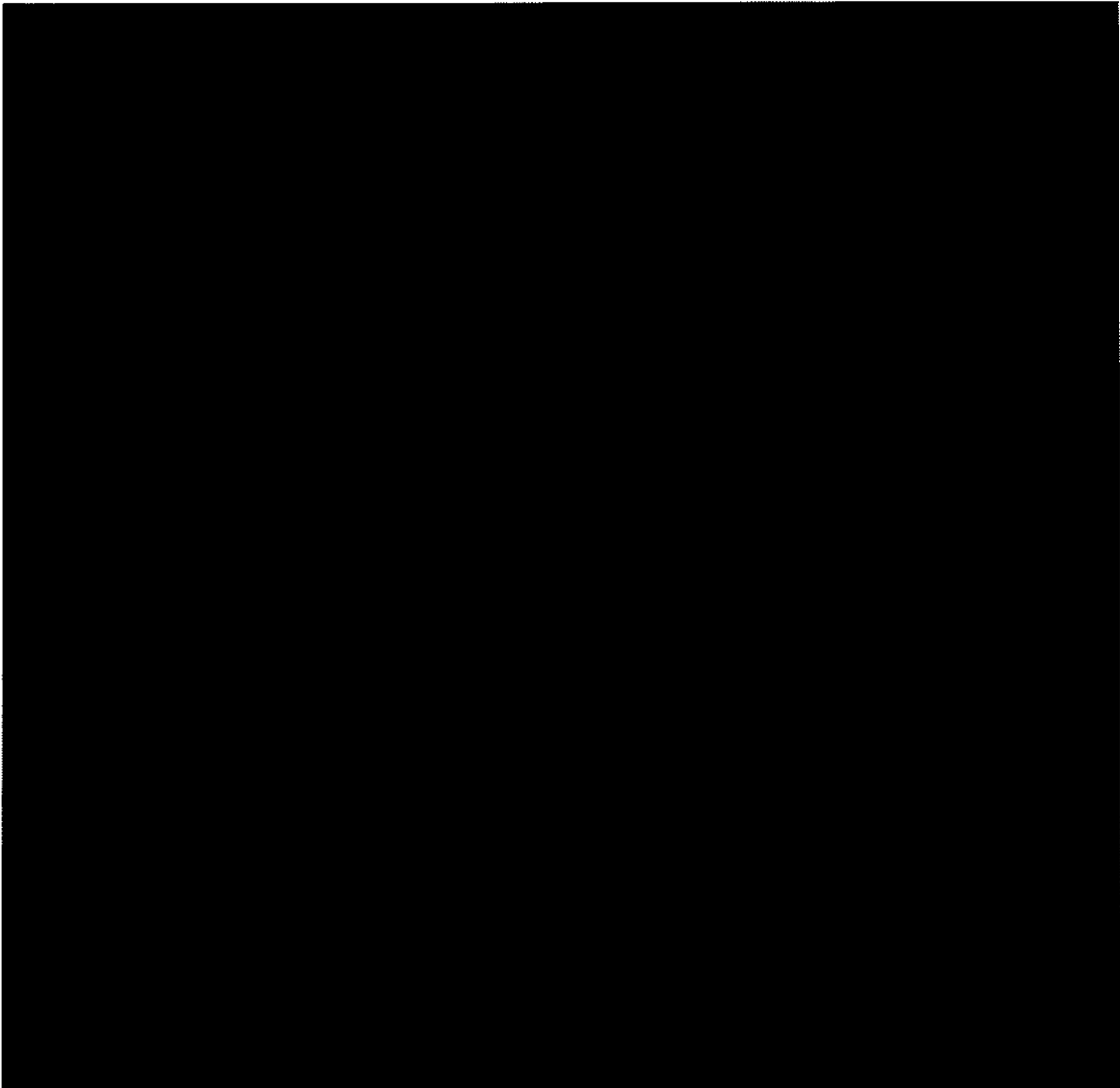
~~TOP SECRET//HUMINT//COMINT//NOFORN~~

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



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

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



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

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

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



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

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

[REDACTED]

As this Court is aware, Court-authorized electronic surveillance of agents of [REDACTED]

[REDACTED]

[REDACTED] Rather than filing

individual applications under title I each time the Government has probable cause to believe that a particular telephone number or e-mail address is being used or is about to be used by members or agents of [REDACTED] targets, the Court would determine that there is probable cause to believe that each of the targets qualifies under FISA as a foreign power that there is probable cause to believe is using or is about to use the specified facilities. The Government would then have the authority pursuant to FISA to direct surveillance at these facilities but would carefully apply stringent minimization procedures to target for collection communications [REDACTED]

[REDACTED] only when there is probable cause to believe: (1) that one of the communicants is a member or agent of [REDACTED] targeted foreign powers, and (2) that the communication is to or from a foreign country. The Government would inform this Court twice a week of any telephone numbers and e-mail addresses that are reasonably believed to be used by a person in the United States, and the collection of communications to or from such numbers and addresses

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

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

could not continue without the explicit approval of this Court. Moreover, such numbers and addresses could not be tasked without the prior approval of the Attorney General, the Assistant Attorney General for the National Security Division, or the Deputy Assistant Attorney General in the National Security Division with responsibility for FISA operations and oversight. For telephone numbers and e-mail addresses that are not reasonably believed to be used by a person in the United States, the Government would submit a report to the Court every thirty days discussing the basis for their selection. At any time, the Court could direct that collection of communications to and from one or more of those non-U.S. numbers or addresses shall cease within forty-eight hours.

I. The Authority Sought in the Application is Critical to the Government's Efforts to Prevent Terrorist Attacks by [REDACTED]

As compared to filing [REDACTED] individual applications under FISA, the approach detailed in the Application, which also complies with and follows the procedures of FISA, would greatly enhance the speed and flexibility with which the Government could use FISA to follow up on new leads to find enemy operatives and allow the Government to obtain actionable intelligence information that otherwise would be lost. For example, if [REDACTED]

[REDACTED]

See NCTC Declaration ¶ 152. Similarly, if the

Government obtains information suggesting there is probable cause to believe that a particular

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

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

telephone number or e-mail address is being used by [REDACTED] time is of the essence—by the time Court or Attorney General authorization to direct surveillance against the particular account is obtained, the account may no longer be in use. *See* NSA Declaration ¶ 23; *see also* NCTC Declaration ¶ 86 (noting that [REDACTED] “employ a range of evasive techniques aimed at making their telephone communications more difficult to intercept and understand” when using telephones to communicate).

Granting the Application would enable the Government to direct electronic surveillance with a much higher degree of speed and agility than would be possible through the filing of individual FISA applications. The authority sought in the Application would thereby prevent the loss of significant actionable intelligence by increasing the speed and flexibility with which the Government could use FISA to follow up on new leads to find operatives of the [REDACTED] foreign powers. In addition, granting the Application would make it possible to collect communications to and from a substantial number of telephone numbers or e-mail addresses being used by such operatives who otherwise would not be surveilled due to resource constraints. The approach detailed in the Application squarely fits within the parameters of FISA because there is probable cause to believe both that the targets are foreign powers and that each of the targets is using, or is about to use, [REDACTED] telephonic and electronic communications. Finally, minimization procedures would be scrupulously applied to target collection at communications that originate or terminate in a foreign country and that are to or from individuals reasonably believed to be operatives of [REDACTED] targeted foreign powers.

Moreover, it was this Court’s ground breaking decision in [REDACTED] that laid the necessary foundation for the attached Application. The innovative legal approach adopted in that

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

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

opinion recognized the significant changes in the way individuals communicate and in the technology that transmits those communications, caused in large part by the advance of the Internet. See, e.g., *id.* at 34-35; 40-42. Keeping in step with those technological changes, the Court authorized the collection under FISA of the meta data associated with an unprecedented number of electronic communications [REDACTED] *Id.* at 39. Like the surveillance approved in [REDACTED] the attached Application describes a novel approach to the challenges created by [REDACTED]

[REDACTED] But the surveillance detailed in the Application involves targeting for collection a much narrower set of communications—only those for which there is probable cause to believe: (1) that one of the communicants is a member or agent of one of the targeted foreign powers and (2) that the communication is to or from a foreign country.

II. The Application Fully Complies with All Statutory Requirements

Section 104 of FISA requires that each application for an order approving electronic surveillance under FISA include:

- (1) the identity of the Federal officer making the application;
- (2) the authority conferred on the Attorney General by the President, and the approval of the Attorney General, to make the application;
- (3) the identity, if known, or a description of the target of the electronic surveillance;
- (4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and (B) each of the facilities or places at which the electronic surveillance is being directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (5) a statement of the proposed minimization procedures;

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

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

- (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (7) a certification by a high-level national security official or officials that the information sought is foreign intelligence information; that a significant purpose of the surveillance is to obtain foreign intelligence information; that such information cannot reasonably be obtained by normal investigative techniques; that designates the information being sought according to the categories set forth in section 101(e) of FISA; and that includes a statement of the basis for the certification that the information sought is the type of foreign intelligence information so designated, and that such information may not be reasonably obtained by normal investigative techniques;
- (8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
- (9) a statement of the facts concerning all previous applications that have been made under title I to the FISA court involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;
- (10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under FISA should not automatically terminate when the described information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and
- (11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

See 50 U.S.C. § 1804(a). In addition to approving the filing of the application, the Attorney General must also find that the application itself meets the requirements of FISA. *Id.*

The attached Application meets these statutory requirements. For the most part, the Application contains material that is either substantially similar to information contained in previous applications approved by this Court (e.g., the nature of the information sought, details regarding prior FISA applications regarding [REDACTED], or that is technical in nature (i.e., the means by which the surveillance will be effected, the coverage of the surveillance devices involved). We need not discuss in

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

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

detail each required element of an application under title I of FISA. Rather, this memorandum will focus on the three aspects of the Application that merit substantial treatment—the targets of the surveillance, the facilities at which the electronic surveillance would be directed, and the minimization procedures.

A. The Targets

Section 104 of FISA requires an application for authorization to conduct electronic surveillance under title I of FISA to specify the identity, if known, of the target of the proposed electronic surveillance, 50 U.S.C. § 1804(a)(3), and to include a statement of “the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power,” *id.* § 1804(a)(4). Similarly, section 105 of FISA requires the Court’s order approving the electronic surveillance to specify the identity, if known, of the target of electronic surveillance. *Id.* § 1805(c)(1)(A). Prior to issuing the order, the Court must find that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *Id.* § 1805(a)(3)(A). With respect to a U.S. person, the probable cause determination may not be predicated solely on activities protected by the First Amendment. *Id.* FISA expressly permits the Court, in determining whether probable cause exists, to consider “past activities of the target, as well as facts and circumstances relating to current or future activities of the target.” *Id.* § 1805(b).

In this case, the United States knows the identity of the targets of the electronic surveillance. As indicated in the Application, [REDACTED]

[REDACTED] The NCTC Declaration specifically describes the known terrorist organizations that [REDACTED]

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

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

[REDACTED] and demonstrates that there is probable cause to believe that, considered together, [REDACTED]

[REDACTED] qualify as a foreign power.⁶

Under FISA, the phrase "foreign power" includes "a group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4). FISA defines as "international terrorism" activities that meet three requirements, *i.e.*, activities that

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
- (2) appear to be intended—(A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Id. § 1801(c). With respect to the first requirement, FISA's legislative history explains that "the violent acts covered by the definition mean both violence to persons and grave or serious violence to property." H.R. Conf. Rep. No. 95-1720, at 21 (1978). Examples of activities that would meet the second requirement include "the detonation of bombs in a metropolitan area, the kidnapping of a high-ranking government official, the hijacking of an airplane in a deliberate and

6

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

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

articulated effort to force the government to release a certain class of prisoners or to suspend aid to a particular country, the deliberate assassination of persons to strike fear into others to deter them from exercising their rights or the destruction of vital governmental facilities." H.R. Rep. No. 95-1283, Pt. I, at 45 (1978); S. Rep. No. 95-701, at 30 (1978) (same). That list is not exclusive. *Id.* The purpose of the third requirement was to ensure that the definition would not include domestic terrorist groups that engage in activities "of a purely domestic nature." H.R. Rep. No. 95-1283, Pt. I, at 30; *see also id.* at 46. Finally, the phrase "activities in preparation" for international terrorism encompasses "activities supportive of acts of serious violence—for example, purchase, or surreptitious importation into [sic] United States of explosives, planning for assassinations or financing of or training for such activities." *Id.* at 42-43.

FISA does not define the term "group," but its ordinary meaning is "[a] number of persons or things regarded as forming a unity on account of any kind of mutual or common relation, or classed together on account of a certain degree of similarity." VI *The Oxford English Dictionary* 887 (2d ed. 1989); *see also American Heritage Dictionary* 800 (3d ed. 1992) ("group" means "[a] number of individuals or things considered together because of similarities"). As the legislative history of FISA recognizes, due to the somewhat amorphous nature of international terrorism, a "group engaged in international terrorism" may be loosely defined. *See* H.R. Rep. No. 95-1283, Pt. I, at 30 (rejecting a requirement that such a group be "foreign-based" because, "in the world of international terrorism[,] a group often does not have a particular 'base,' or if it does, it may be nearly impossible to discern").

The facts and circumstances detailed in the NCTC Declaration demonstrate that there is probable cause to believe that [REDACTED] is a group that is engaged in international terrorism or in preparatory activities therefor. As the Supreme Court

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

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

has recently explained, "[t]he probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Rather than being "technical," these probabilities "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar v. United States*, 338 U.S. 160, 176 (1949). In addition, probable cause "does not require the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance standard demands." *Gerstein v. Pugh*, 420 U.S. 103, 121 (1975); see also *Illinois v. Gates*, 462 U.S. 213, 235 (1983) ("Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the [probable cause] decision.")⁷

Evaluated against the backdrop of the Supreme Court's guidance on applying the probable cause standard, the evidence clearly demonstrates that there is probable cause to believe that [REDACTED] is a group engaged in international terrorism or in activities in preparation therefor, and thus is a foreign power under FISA. [REDACTED]

⁷ We note that the showing of "probable cause" required to obtain an order from this Court may be "less than the traditional probable cause standard for the issuance of a search warrant" because the application for such an order is made "in the context of foreign intelligence." *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); see also H.R. Rep. No. 95-1283, Pt. I, at 79 ("probable cause" standard in FISA is not the ordinary "probable cause" that a crime is being committed which applies to searches and seizures for law enforcement purposes); cf. *United States v. United States District Court (Keith)*, 407 U.S. 297, 322-23 (1972) (Fourth Amendment may permit Congress to impose standards on surveillance for domestic security purposes that are different from the standards prescribed by Title III if the new standards "are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."). But cf. H.R. Rep. No. 95-1283, Pt. I, at 30 (unlike some of the other definitions of a "foreign power," "the term 'international terrorism' is a defined term . . . and includes within it a criminal standard"). We need not rely on that argument here, however. There is ample evidence to demonstrate that under even the more demanding standard, there is probable cause to believe that [REDACTED] is a group engaged in international terrorism or in activities in preparation therefor.

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

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

and b(7)(E)

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

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

8

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

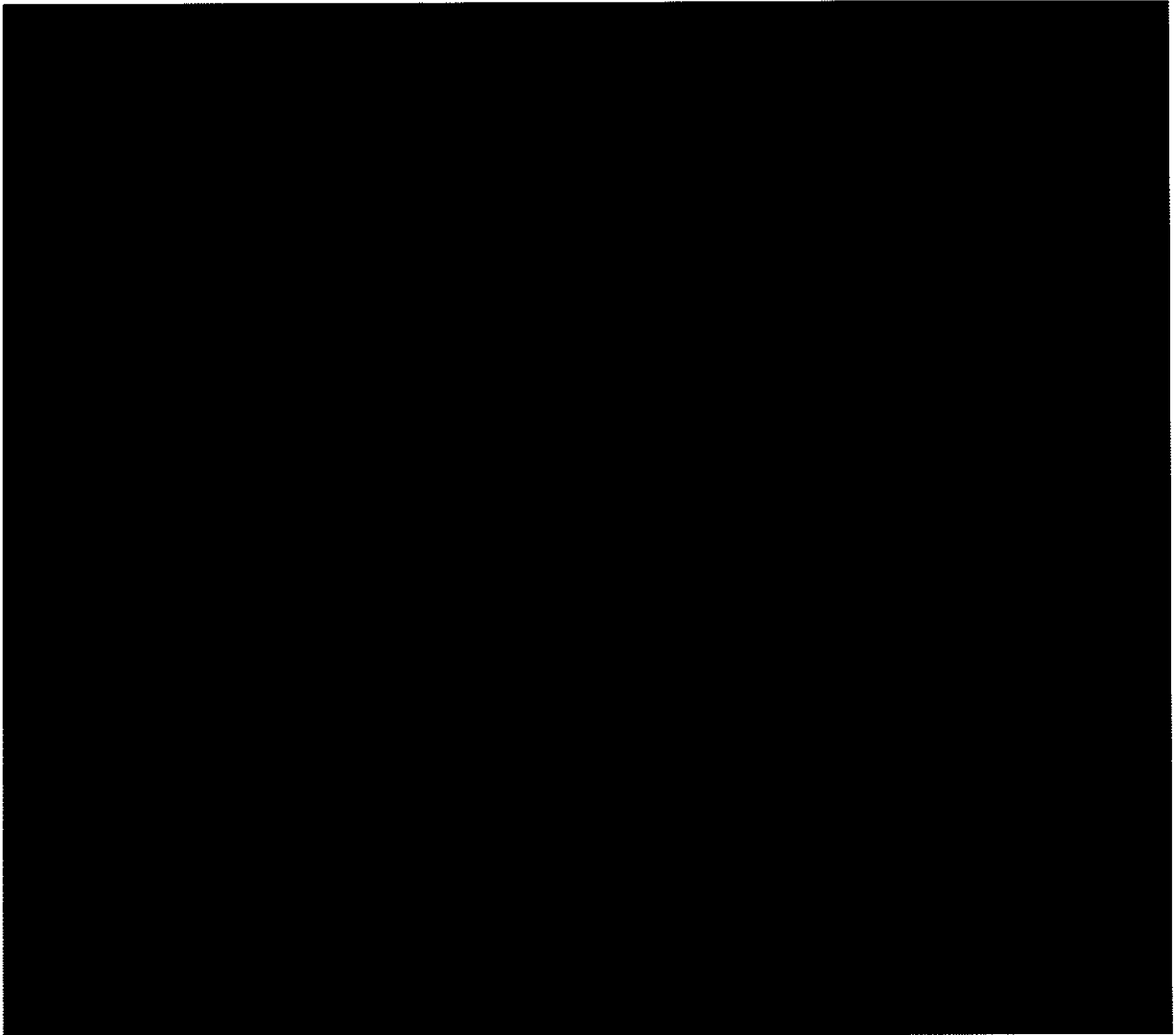
~~TOP SECRET//HUMINT//COMINT//NOFORN~~

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



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

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



9



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

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

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



B. The Facilities

FISA requires that each application under title I of the Act 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). And this

10



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

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

Court may approve the surveillance only if it finds, on the basis of the facts submitted by the applicant, that there is probable cause for that belief. *Id.* § 1805(a)(3)(B). In making that determination, FISA expressly permits the Court to consider "past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Id.* § 1805(b). In addition to finding probable cause, 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). Taking these requirements in reverse order, the attached Application both specifies the nature and location of each of the facilities or places at which the electronic surveillance will be directed and establishes that there is probable cause to believe that such facilities or places are being used, or are about to be used, by a foreign power or its agents—namely, [REDACTED]

1. *Identifying the Facilities*

The terms "facility" and "place" are broad. Because FISA does not define these terms, we look to their ordinary meaning. See *Walters v. Metropolitan Ed. Enterprises, Inc.*, 519 U.S. 202, 207 (1997) ("In the absence of an indication to the contrary, words in a statute are assumed to bear their ordinary, contemporary, common meaning.") (quotations and citations omitted); see also *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). "Facility" means "[s]omething that facilitates an action or process" or "[s]omething created to serve a particular function." *American Heritage Dictionary* 653 (3d ed. 1992); see also *The Oxford English Dictionary* 649 (2d ed. 1989)

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

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

(defining "facility" as "the physical means for doing something"); *Funk & Wagnalls New Standard Dictionary of the English Language* 888 (1946) ("facility" means "[s]omething by which anything is made easier or less difficult; an aid, advantage, or convenience"). "Place" is defined as "[a]n area with definite or indefinite boundaries; a portion of space. . . . The particular portion of space occupied by or allocated to a person or thing." *American Heritage Dictionary* 1382 (3d ed. 1992); see also XI *The Oxford English Dictionary* 937 (2d ed. 1989) (defining "place" as "[a] particular part of space, of defined or undefined extent, but of definite situation"); *Funk & Wagnalls New Standard Dictionary of the English Language* 1889 (1946) ("place" means "[a] particular point or portion of space").¹¹

As detailed in the Application, the "facilities or places" at which the electronic surveillance would be directed would be: (1) for telephone calls, [REDACTED]

[REDACTED]

¹¹ Although there is little legislative history at the time of enactment of FISA regarding how Congress intended the phrase "facilities or places" to be read, there is more recent legislative history indicating that Congress may have recognized that, particularly with the advent of the Internet, the phrase should be considered broadly. In 2001, in the context of discussing an amendment that added the phrase "if known" to the requirement in section 105(c)(1)(B) of FISA that the court's order specify "the nature and location of the facilities or places at which the electronic surveillance will be directed," see Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a)(2), 115 Stat. 1394, 1402 (2001), Congress noted that "[o]bviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations." See H.R. Conf. Rep. No. 107-328, at 24 (2001). Thus, there is strong evidence that, at least in 2001, Congress understood the phrase "facilities or places" broadly to include the multitude of locations at which electronic communications may be accessed.

¹² [REDACTED]

¹³ For ease of discussion, this memorandum will use the phrase [REDACTED]

[REDACTED]

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

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

[REDACTED]
[REDACTED] and (2) for e-mails, [REDACTED]
[REDACTED]

14 [REDACTED]
[REDACTED]

¹⁵ Significantly, other parts of the United States Code dealing with electronic surveillance and pen registers and trap and trace devices use the term "facilities" consistent with this broad understanding. See, e.g., 18 U.S.C. § 2510(1) (defining "wire communication" as "any aural transfer made . . . through the use of facilities for the transmission of communications" using certain types of connections [REDACTED]; *id.* § 2510(14) (defining "electronic communications system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications"); *but cf. id.* § 2518(3)(d) (with certain exceptions, requiring a court order under Title III to find probable cause that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are . . . leased to; listed in the name of, or commonly used by" the individual committing the crime). In addition, section 216 of the USA PATRIOT Act amended the definition of "pen register" in 18 U.S.C. § 3127(3) to include information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." Pub. L. No. 107-56, § 216(c)(3), 115 Stat. 272, 290 (2001) (emphasis added). The legislative history of the PATRIOT Act indicates that the purpose of that amendment was to ensure that the pen register provision applied "to facilities other than telephone lines (e.g., the Internet)." 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (section-by-section analysis entered into the record by Sen. Leahy). Thus, at least in 2001, Congress envisioned that the term "facilities" was broad enough to encompass the entire Internet.

[REDACTED]

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

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

[REDACTED] and b(6), b(7)(A), (C), and (E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

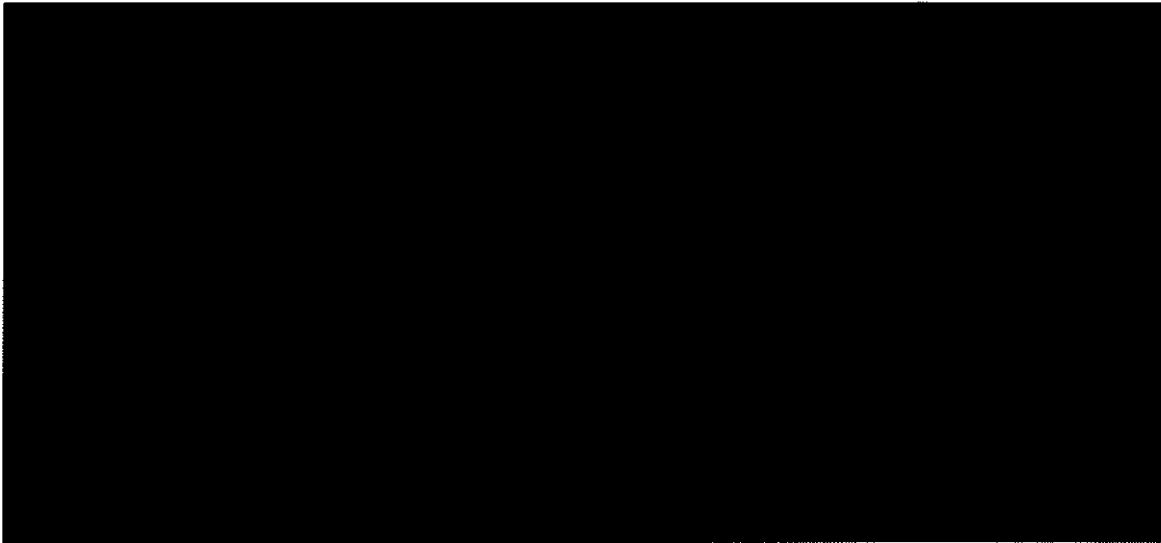
In the context of title IV of FISA, this Court discussed the requirement in section 402(d)(2)(A)(ii) that its order specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(A)(ii). This Court found that the language of this provision, which includes the phrase "or other facility," did not require that a pen register be attached only to a facility associated with a particular individual. See [REDACTED] at 21-23.¹⁶ In making that finding, this Court recognized that its conclusion meant that FISA "encompass[es] an exceptionally broad form of collection." *Id.* at 23. Nonetheless, it described as "facilities" [REDACTED]

[REDACTED]

¹⁶ That finding is particularly significant because section 402(d)(2)(A)(ii) describes the "other facility" far more narrowly than section 105(c)(1)(B), seeming explicitly to link the phrase "other facility" to the identity (if known) of a particular person, *i.e.*, the "person to whom [it] is leased or in whose name [it] is listed." 50 U.S.C. § 1842(d)(2)(A)(ii). In contrast, section 105(c)(1)(B) refers broadly to "the facilities or places at which the electronic surveillance will be directed, if known." *Id.* § 1805(c)(1)(B).

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

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



We recognize that this Court has cautioned that the authorization of bulk collection of meta data from electronic communications should not be relied on as a precedent for similar collection of the substantive contents of communications under title I of FISA. See [REDACTED] [REDACTED] Order at 49, n.34. The electronic surveillance proposed in the attached Application, however, is not similar to the bulk collection approved in that case because it would be narrowly circumscribed and focused. In view of the proposed minimization procedures, the Application seeks authorization from this Court to target for collection the contents of communications only if there is probable cause to believe that (1) one of the parties to the communication is a member or agent of [REDACTED] target, *i.e.*, [REDACTED] [REDACTED] and (2) one end of the communication is in a foreign country. Although [REDACTED] certainly did not address the type of surveillance presented here, the decision was critical to laying the foundation for this Application.

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

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

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

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



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

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

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



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



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

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

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



and b(7)(E)



and b(7)(E)



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

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

[REDACTED] here, although electronic surveillance would be directed at "facilities" that, consistent with the term's ordinary and natural meaning, would not be limited to particular telephone numbers or e-mail addresses, the Government would apply strict minimization procedures to target for collection only communications to or from those specific telephone numbers and e-mail addresses for which there is probable cause to believe that (1) one of the parties to the communication is a member or agent of [REDACTED] and (2) that the communication is to or from a foreign country. Although the telephone numbers and e-mail addresses are not presented in the Application for the Court's approval, the Government will target for collection only communications to or from specific telephone numbers and e-mail addresses determined to be associated with the [REDACTED] foreign powers. Moreover, the Government will continue to collect communications to and from telephone numbers and e-mail addresses reasonably believed to be used by a person in the United States only with the explicit and prompt approval of the Court, and at least every 30 days the Court will have the opportunity to review the basis for tasking telephone numbers and e-mail addresses not reasonably believed to be used by a person in the United States and to direct the collection to cease if the Court believes that the minimization probable cause standard is not met.

[REDACTED]

¹⁸ Although the term "facility" is certainly broad enough to include [REDACTED] its plain meaning also includes the specific telephone numbers and e-mail addresses with respect to which the Government routinely seeks this Court's authorization to conduct electronic surveillance. Specific telephone numbers and e-mail addresses also qualify as "facilities" under FISA because they also facilitate the transmission of communications.

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

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

[REDACTED]

Under section 105(a)(3)(B) of FISA, the Court's order must find 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. § 1805(a)(3)(B). As relevant here, FISA defines "electronic surveillance" to include "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States" *Id.* § 1801(f)(2). Here, a surveillance device in the United States will be used to acquire the contents of wire communications to or from persons in the United States. The proposed electronic surveillance would be [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

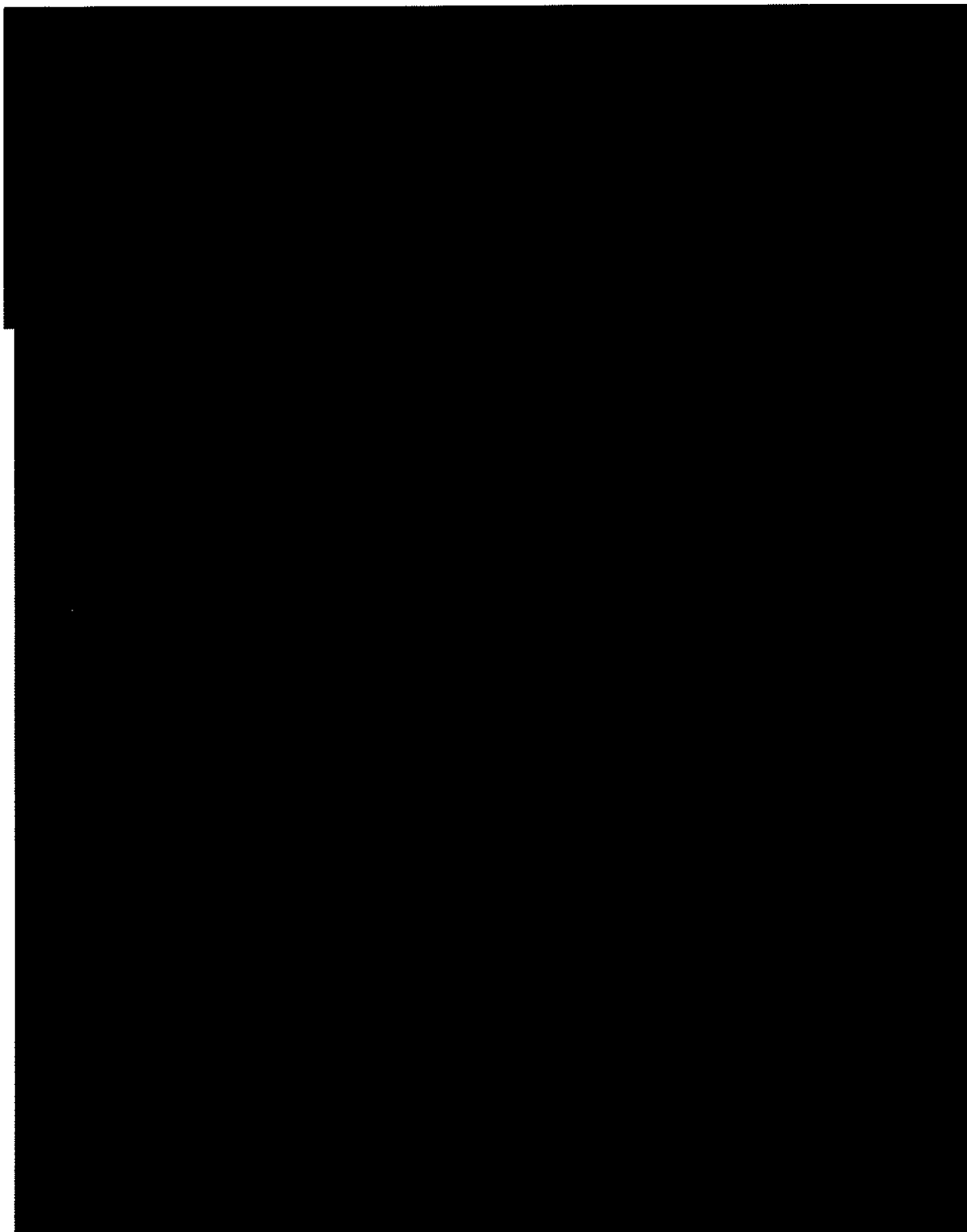
~~TOP SECRET//HUMINT//COMINT//NOFORN~~[REDACTED] and b(6), b(7)(A), (C), and (E)
[REDACTED]
[REDACTED]
[REDACTED]

2. *Establishing Probable Cause for Use of the Facilities*

The NSA Declaration demonstrates that there is probable cause to believe that each of the facilities listed in the Application is being used, or is about to be used, by a foreign power or its agents. As noted by the Court of Review, FISA does not require a particularly strong nexus between the facilities and the type of communications that they carry. *See In re Sealed Case*, 310 F.3d 717, 740 (For. Intell. Surv. Ct. of Rev. 2002) ("Simply put, FISA requires less of a nexus between the facility and the pertinent communications than Title III."). In contrast to the Title III (ordinary criminal law enforcement) regime, the Court need not find probable cause to believe that the facilities are being used, or are about to be used, in connection with a criminal offense. *Cf.* 18 U.S.C. § 2518(3)(d) (requiring such a finding if the targeted facilities are not leased to, listed in the name of, or used by the individual committing the crime). Instead, the Court need only find probable cause to believe that the facilities are being used, or are about to be used, by a foreign power or an agent of a foreign power. And, in determining whether probable cause exists, FISA expressly permits the Court to consider "past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b).

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

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



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

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

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

[REDACTED] a vast proportion of the world's Internet traffic is
carried at some point on the communications infrastructure in the United States. b(1), b(7)(E)

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

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

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

traffic. NSA Declaration ¶ 7.

[REDACTED]

[REDACTED]

C. The Minimization Procedures

[REDACTED]

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

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

[REDACTED] We emphasize, however, that the Government has no interest in obtaining all communications [REDACTED]

[REDACTED] or anything remotely approaching that amount. To the contrary, the Government would not collect more information than is necessary. Instead, minimization procedures would be applied that would ensure that communications would be targeted for collection only if there is probable cause to believe¹⁹ that: (1) one of the parties to the communication is a member or agent of [REDACTED]

[REDACTED] and (2) the communication is to or from a foreign country. See 50 U.S.C. § 1804(a)(5) (requiring that the Government's application include "a statement of the proposed minimization procedures").²⁰

In particular, the NSA would collect the contents of communications to or from a particular telephone number only if there is probable cause to believe that the telephone number is used by a member or agent of [REDACTED]

¹⁹ As a practical matter, NSA lawyers would explain the minimization probable cause standard to relevant officials as being equivalent to a determination, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are reasonable grounds to believe that (1) one of the communicants is a member or agent of [REDACTED] and (2) the communication is to or from a foreign country. NSA Declaration ¶ 18, n.20. The "reasonable grounds to believe" standard is simply a different way of articulating the probable cause standard. As the Supreme Court has explained, "[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt." *Maryland v. Pringle*, 540 U.S. at 371 (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949)). The Court has stated, moreover, that such a reasonable ground for belief must be based on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar*, 338 U.S. at 175; see also *Pringle*, 540 U.S. at 370 (quoting *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quoting *Brinegar*)); *United States v. Bennett*, 905 F.2d 931, 934 (6th Cir. 1990) ("Probable cause is defined as reasonable grounds for belief . . .") (internal quotation marks omitted); cf. 18 U.S.C. § 3050 (authorizing Bureau of Prisons officers to make warrantless arrests when they have "reasonable grounds to believe that the arrested person is guilty" of the offense for which he is being arrested). Thus, the "reasonable grounds to believe" standard draws upon the precise terms that the courts have used to describe the probable cause standard.

²⁰ The Application also proposes that the NSA would follow their standard minimization procedures for electronic surveillance on file with the Court. See United States Signals Intelligence Directive 18 ("USSID 18"), Annex A, App. 1 (1993 & 1997) ("NSA Standard Minimization Procedures"). This Court has already found on multiple occasions that the NSA Standard Minimization Procedures satisfy the definition of minimization procedures set forth in section 101(h) of FISA.

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

~~TOP SECRET//SI//MINT//COMINT//NOFORN~~

[REDACTED] Similarly, if there is probable cause to believe that an e-mail address is used by a member or agent of [REDACTED] the NSA would collect the contents of communications either to or from that e-mail address, or that mention the specific e-mail address in the body of the message. In addition, the NSA would rely on a variety of methods to ensure that there is probable cause to believe that one end of the collected communications would be foreign. For example, [REDACTED]

[REDACTED]

[REDACTED]

Technically, the collection of e-mail messages that meet the minimization probable cause standard would typically be accomplished as follows: [REDACTED]

[REDACTED]

21 [REDACTED]

22 [REDACTED]

~~TOP SECRET//SI//MINT//COMINT//NOFORN~~

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

[REDACTED]

[REDACTED] Moreover, the Government would inform this Court twice a week of any telephone numbers and e-mail addresses reasonably believed to be used by a person in the United States, and the collection of communications to or from those numbers or addresses could not continue without the explicit approval of this Court. And such numbers and addresses could not be tasked without the prior approval of the Attorney General, the Assistant Attorney General for the National Security Division, or the Deputy Assistant Attorney General in the National Security Division with responsibility for FISA operations and oversight. For telephone numbers and e-mail addresses that are not reasonably believed to be used by a person in the United States, the Government would submit a report to the Court every thirty days discussing the basis for their selection. At any time, the Court could direct that the collection of communications to and from one or more

23

[REDACTED]

24

[REDACTED]

25

[REDACTED]

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

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

of those non-U.S. numbers or addresses shall cease within forty-eight hours. Finally, with every application to renew this authorization, the Government would explain its current understanding of which specific terrorist organizations are associated with [REDACTED]

One of the preconditions to the Court's approving an application for electronic surveillance is that the proposed minimization procedures meet the definition of minimization procedures under section 101(h) of FISA. *See* 50 U.S.C. § 1805(a)(4). The Application meets that criterion. According to the portion of section 101(h) that is relevant here, 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." *Id.* § 1801(h)(1).²⁶ The plain text of the definition indicates that, when appropriate, minimization procedures may be applied to the acquisition of information, as well as to its retention and dissemination. This statutory language suggests that Congress contemplated that, perhaps due to the potentially broad application of the term "facility," minimization procedures would sometimes be necessary to narrow the potential acquisition of information obtained through electronic surveillance. Indeed, as the Court of Review pointed out, "[b]y minimizing acquisition, Congress envisioned that, for example, 'where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party' to the communication." *In re Sealed Case*, 310 F.3d at 731

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

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

of those non-U.S. numbers or addresses shall cease within forty-eight hours. Finally, with every application to renew this authorization, the Government would explain its current understanding of which specific terrorist organizations are associated with [REDACTED]

One of the preconditions to the Court's approving an application for electronic surveillance is that the proposed minimization procedures meet the definition of minimization procedures under section 101(h) of FISA. *See* 50 U.S.C. § 1805(a)(4). The Application meets that criterion. According to the portion of section 101(h) that is relevant here, 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." *Id.* § 1801(h)(1).²⁶ The plain text of the definition indicates that, when appropriate, minimization procedures may be applied to the acquisition of information, as well as to its retention and dissemination. This statutory language suggests that Congress contemplated that, perhaps due to the potentially broad application of the term "facility," minimization procedures would sometimes be necessary to narrow the potential acquisition of information obtained through electronic surveillance. Indeed, as the Court of Review pointed out, "[b]y minimizing acquisition, Congress envisioned that, for example, 'where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party' to the communication." *In re Sealed Case*, 310 F.3d at 731

²⁶ The Attorney General has adopted these new minimization procedures by virtue of his approval of the attached Application. *Cf. In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets*, Motion for Amended Orders Permitting Modified Minimization Procedures, No. [REDACTED] at 8 (May 10, 2002) ("Raw Take Motion").

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

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

(quoting H.R. Rep. No. 95-1283, Pt. I, at 55-56 (1978)) (emphasis in original);

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

There have been several occasions on which this Court has authorized the Government to conduct electronic surveillance that includes minimization at the time of acquisition. *Cf.* 310 F.3d at 740 (noting that in the FISA context, minimization usually occurs at the retention, rather than the acquisition stage—"in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent

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

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

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

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



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

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

and b(7)(E)



27

and b(7)(E)




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

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

(and b(7)(E))

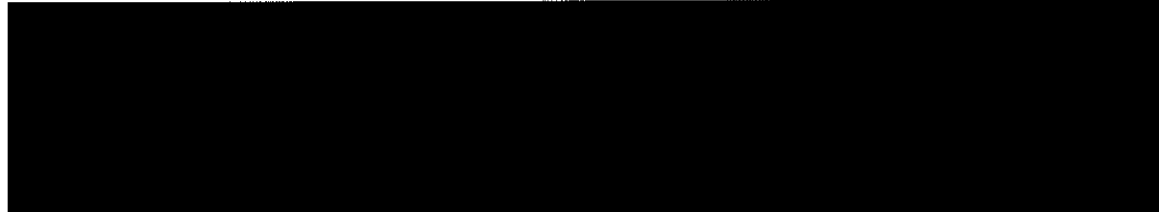
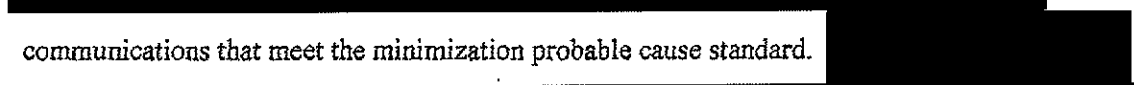


The surveillance detailed in the attached Application would involve the "acquisition" by the Government of the contents of



only

communications that meet the minimization probable cause standard.



28



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

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

[REDACTED] that would be reviewed by a human being at NSA would be communications to or from telephone numbers or e-mail addresses if two conditions are met, i.e., there is probable cause to believe that: (1) the telephone number or e-mail address is associated with [REDACTED] targeted foreign powers; and (2) one end of the communication is in a foreign country. Communications that do not meet these criteria would not be targeted for collection.

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



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

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

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



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



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



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

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



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



In addition to the particularized minimization procedures designed to acquire only the international communications of individuals who are members or agents of   the NSA will also apply the existing "NSA Standard Minimization Procedures" that are already on file with the Court. *See supra* n.19. For example, the NSA Standard Minimization Procedures require that analysts "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 as either clearly not relevant to the authorized purpose of the surveillance . . . or as containing evidence of a crime." NSA Standard Minimization Procedures § 3(c)(2).

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

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

Here, collection would be targeted at communications to or from telephone numbers or e-mail addresses if there is probable cause to believe that: (1) the telephone number or e-mail address is associated with [REDACTED] targeted foreign powers; and (2) one end of the communication is in a foreign country. Under the Order sought in this Application, NSA must and will capitalize [REDACTED]

[REDACTED]

[REDACTED] As noted above, for reasons of technical feasibility relating to the capabilities of NSA's worldwide signals intelligence systems, there is some unavoidable incidental collection with respect to e-mail communications. *Id.* [REDACTED]

[REDACTED]

The NSA will respond to this incidental collection in three ways. First, in deciding whether to task a particular e-mail address, analysts will weigh the possibility that tasking the e-mail address could lead to incidental collection against the counterterrorism need to collect the communications of that address. *Id.* Second, the collection generally will be focused on [REDACTED]

[REDACTED]

30

[REDACTED]

NSA Declaration ¶ 19 n.22.

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

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

[REDACTED] *Id.* Third, any incidentally collected communications will be treated in accordance with the NSA Standard Minimization Procedures. *Id.* In light of the fact that it is not currently technically feasible for the NSA to avoid the incidental collection described herein, these specific constraints “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.” 50 U.S.C. § 1801(h)(1).

The Government will apply several additional mechanisms to ensure appropriate oversight over the collection of communications under this authorization. If the telephone number or e-mail address tasked for collection is reasonably believed to be used by a person in the United States, six specific procedures will be followed.

- First, only three senior NSA officials will be authorized by the Director of the NSA to approve tasking the number or address for collection—the Signals Intelligence Directorate Program Manager for Special Counterterrorism Projects, the Counterterrorism Global Capabilities Manager, and the Counterterrorism Primary Production Center Manager.
- Second, all such authorizations will be documented in writing and supported by a written justification explaining why the selected telephone numbers or e-mail addresses meet the minimization probable cause standard.
- Third, the number or e-mail address may not be tasked for collection without the prior approval of the Attorney General, the Assistant Attorney General for the National Security Division (AAG/NSD), or the Deputy Assistant Attorney General in the National Security Division with responsibility for FISA operations and oversight (DAAG).
- Fourth, no such telephone number or e-mail address may be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.

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

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

- Fifth, tasking such phone numbers and e-mail addresses for collection must be explicitly approved by this Court.
 - The Government will report to the Court twice a week on any new numbers or addresses that are reasonably believed to be used by persons in the United States. Included within each report will be a description of the basis for the determination by the NSA and the Attorney General, the AAG/NSD, or the DAAG that there was probable cause to believe that the number or address is associated with a member or agent of [REDACTED]
 - If the Court does not approve any of the new telephone numbers or e-mail addresses within forty-eight hours of receiving the report because the Court does not agree that there is probable cause to believe that the number or address is associated with a member or agent of [REDACTED] the Government would have twenty-four hours to submit additional information.
 - If the Court does not, within twenty-four hours of receiving additional information from the Government, find that there is probable cause to believe that any of the new telephone numbers or e-mail addresses is associated with a member or agent of [REDACTED] the tasking of that number or address must cease and any acquired communications must be segregated and may be retained only upon Court approval if the Government demonstrates a foreign intelligence need for such retention.
- Finally, the NSA will institute a system that ensures that telephone numbers and e-mail addresses of persons reasonably believed to be in the United States will be reviewed every 90 days to determine whether surveillance of the number or address should continue.

See NSA Declaration ¶ 68.³¹

Telephone numbers and e-mail addresses not reasonably believed to be used by a person in the United States will be tasked only after an NSA analyst has documented in writing why the number or address meets the minimization probable cause standard and an official in the NSA's

[REDACTED] Branch has verified that the analyst's

³¹ At this time, for operational reasons, it is not anticipated that the NSA will, under the authority sought in the Application, task for collection any e-mail addresses reasonably believed to be used by a person in the United States.

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

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

determination has been properly documented. *Id.* ¶ 67. In addition, an attorney from the National Security Division at the Department of Justice will review the NSA's justifications for targeting these numbers and addresses. Every thirty days, the Government will submit a report to the Court listing new numbers and addresses that are not reasonably believed to be used by persons in the United States and that the NSA has tasked during the previous thirty days and briefly summarizing the basis for the NSA's determination that there was probable cause to believe that each number and address is associated with a member or agent of [REDACTED]

[REDACTED] At any time, the Court may request additional information on particular numbers or addresses and, if the Court finds that there is not probable cause to believe that any number or address is associated with a member or agent of [REDACTED]

[REDACTED] the Court may direct the collection of communications to and from that number or address to cease within forty-eight hours. The Court may also direct that any communications acquired using those particular numbers or addresses must be segregated and may be retained only upon Court approval if the Government demonstrates a foreign intelligence need for such retention.

With respect to the program as a whole, the NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate's Office of Oversight and Compliance will each conduct a periodic review. In addition, the Director of the NSA will direct the Inspector General and General Counsel to submit an initial report to him 60 days after the initiation of the collection to assess the efficacy of the management controls and to ensure that the processing and dissemination of U.S. person information is accomplished in accordance with the NSA Standard Minimization Procedures. And the Director of the NSA anticipates that, consistent with direction from the President, he will, in coordination with the Attorney General, inform the

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

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

congressional Intelligence Committees of the Court's approval of this collection activity.

Finally, with every application to renew this authorization, the Government would explain its current understanding of which specific terrorist organizations are associated with [REDACTED]

III. The Application Fully Complies with the Fourth Amendment

As this memorandum establishes, this Court may authorize under FISA the collection of a large number of communications. In addition to the statutory protections discussed above, such as the requirements for specific minimization procedures, the Fourth Amendment is a fundamental safeguard that cabins that authority. The electronic surveillance described in the Application is fully consistent with the Fourth Amendment, which prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether the search is "reasonable." *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) ("As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a government search is 'reasonableness.'"). The warrant requirement does not apply to this case, which involves both the inherent authority of the President to conduct warrantless electronic surveillance to obtain foreign intelligence to protect our Nation from the threat of armed attack and "special needs" beyond the need for ordinary law enforcement. Moreover, the surveillance detailed in the Application is certainly reasonable, particularly taking into account all of the procedural safeguards required by FISA and the nature of the threat faced by the United States.

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

~~TOP SECRET//SI//MINT//COMINT//NOFORN~~

A. The Warrant Requirement of the Fourth Amendment Does Not Apply to the Electronic Surveillance Described in the Application

In “the criminal context,” as the Supreme Court has pointed out, “reasonableness usually requires a showing of probable cause” and a warrant. *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). The warrant requirement, however, is not universal. Rather, the “Fourth Amendment’s central requirement is one of reasonableness,” and the rules the Court has developed to implement that requirement “[s]ometimes . . . require warrants.” *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); *see also Earls*, 536 U.S. at 828 (noting that the probable cause standard “is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions”) (internal quotation marks omitted).

Indeed, the Court of Review has concluded that electronic surveillance conducted pursuant to FISA need not satisfy the warrant requirement. In *In re Sealed Case*, the court held that FISA, as amended by the USA PATRIOT Act, is constitutional. *See* 310 F.3d at 746. The court’s decision, however, was not based on a determination that FISA’s procedures generally satisfy the warrant requirement. Instead, the court expressly reserved whether a FISA order meets the warrant requirement. *See id.* at 741-42 (“[A] FISA order may not be a ‘warrant’ contemplated by the Fourth Amendment We do not decide the issue”); *see also id.* at 744 (“assuming *arguendo* that FISA orders are not Fourth Amendment warrants”); *id.* at 746 (“the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close”). The court described the President’s well-established inherent authority to conduct warrantless searches to obtain foreign intelligence information—“[t]he *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to

~~TOP SECRET//SI//MINT//COMINT//NOFORN~~

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

obtain foreign intelligence information. . . . We take for granted that the President does have that authority” *Id.* at 742. Rather than examining the boundaries of that authority, the court saw its task as focusing on whether “FISA amplif[ies] the President’s power by providing a mechanism that at least approaches a classic warrant.” *Id.* The court also discussed the Supreme Court’s cases that approve “warrantless and even suspicionless searches that are designed to serve the government’s ‘special needs, beyond the normal need for law enforcement.’” *Id.* at 745 (quoting *Vernonia*, 515 U.S. at 653). Although “not dispositive,” the Court of Review concluded that, as with the special needs cases, “FISA’s general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers” was a “crucial factor” in the court’s Fourth Amendment analysis. 310 F.3d at 746. After analyzing FISA’s procedural requirements, the court concluded:

Even without taking into account the President’s inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from [*United States v. United States District Court*, 407 U.S. 297 (1972) (*Keith*)], that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Id. at 746.

Of course, the decision of the Court of Review that FISA is constitutional even if it does not satisfy the Fourth Amendment’s warrant requirement is binding on this Court. The only remaining question under the Fourth Amendment is whether the surveillance detailed in the Application would be reasonable. Nevertheless, before turning to the question of reasonableness, we first elaborate on two important doctrines discussed by the Court of Review:

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

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

the President's inherent authority to collect foreign intelligence without a warrant, and the "special needs" doctrine, which also authorizes warrantless searches.³²

1. The President Has Inherent Authority to Conduct Warrantless Electronic Surveillance to Protect Our National Security from Foreign Threats

It has long been established that the President, as the Commander in Chief of the Armed Forces and the "sole organ of the nation" in the conduct of foreign affairs, *United States v.*

³² Even if the Fourth Amendment's warrant requirement were to apply, it would be satisfied by the Court's issuance of an order under section 105 of FISA authorizing the electronic surveillance detailed in the Application. As the Court of Review has explained:

In the context of ordinary crime, beyond requiring searches and seizures to be reasonable, the Supreme Court has interpreted the warrant clause of the Fourth Amendment to require three elements: "First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense. Finally, warrants must particularly describe the 'things to be seized, as well as the place to be searched.'"

In re Sealed Case, 310 F.3d at 738-39 (quoting *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotations and citations omitted)).

The order requested in the Application would meet those requirements. First, it would be issued by a neutral, disinterested judge. Second, the probable cause standard that would be met satisfies the requirements of the Fourth Amendment. See *United States v. Duggan*, 743 F.2d 59, 72-74 (2d Cir. 1984) (finding that FISA does not violate the probable cause requirement of the Fourth Amendment because its requirements provide an appropriate balance between the individual's interest in privacy and the Government's need to obtain foreign intelligence information); cf. *Keith*, 407 U.S. at 322-23 (advising that, in the domestic security context, "different standards" from those applied to traditional law enforcement "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.") Third, the order would meet the particularity requirement because it would not authorize a general search, but instead would authorize carefully delineated electronic surveillance. The order would sufficiently describe the "things to be seized"—international communications with respect to which there is probable cause to believe that one party is a member or agent of [REDACTED]—and the "place to be searched"—specifically identified facilities or places for which there is probable cause to believe that they are being used, or are about to be used, by these foreign powers. See *United States v. Grubbs*, 126 S. Ct. 1494, 1500 (2006) ("The Fourth Amendment . . . specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and the 'persons or things to be seized.'"). As required by FISA, the order would also specify the identity of the target, the type of information sought to be acquired, the type of communications being subjected to surveillance, and the period for which the surveillance would be authorized. Moreover, the order would direct that certain minimization procedures be applied with respect to the acquisition, retention and dissemination of U.S. person information. Finally, the order would be based upon a certification by a high-level national security officer that the information being sought is foreign intelligence information that cannot be obtained by normal investigative techniques. Thus, we submit that the order would satisfy the requirements of the Warrant Clause, were that clause deemed to apply.

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

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

Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted), has an inherent constitutional authority to conduct warrantless searches for foreign intelligence purposes. See *In re Sealed Case*, 310 F.3d at 746 (noting “the President’s inherent constitutional authority to conduct warrantless foreign intelligence surveillance”); *id.* at 742 (“tak[ing] for granted” that inherent authority); *cf. Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing the President’s authority during the Civil War “to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy”); *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980) (noting that “the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance”). Indeed, as the Court of Review has recognized, 310 F.3d at 742, every federal court that has ruled on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. See, e.g., *Truong*, 629 F.2d 908; *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). But *cf. Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that a warrant would be required even in a foreign intelligence investigation).

To be sure, the Supreme Court has left this precise question open. In *United States v. United States District Court*, 407 U.S. 297 (1972) (*Keith*), the Supreme Court concluded that the Fourth Amendment’s warrant requirement applies to investigations of purely *domestic* threats to security—such as domestic terrorism. The Court made clear, however, that it was not addressing executive authority to conduct *foreign* intelligence surveillance: “[T]he instant case requires no judgment on the scope of the President’s surveillance power with respect to the activities of

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

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

foreign powers, within or without this country." *Id.* at 308; *see also id.* at 321-322 & n.20 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."). Indeed, the Court took note of several sources supporting "the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved." *Id.* at 322 n.20 (citing *United States v. Smith*, 321 F. Supp. 424, 425-26 (C.D. Cal. 1981); ABA Project on Standards for Criminal Justice, Electronic Surveillance 120, 121 (Approved Draft 1971 and Feb. 1971 Supp. 11); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970)).

Indeed, each of the three courts of appeals noted above decided—after *Keith*, and expressly taking *Keith* into account—that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. As the U.S. Court of Appeals for the Fourth Circuit observed in *Truong*, "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities." 629 F.2d at 913 (internal quotation marks omitted). The court pointed out that a warrant requirement would be a hurdle that would reduce the Executive's flexibility in responding to foreign threats that "require the utmost stealth, speed, and secrecy." *Id.* It also would potentially jeopardize security by increasing "the chance of leaks regarding sensitive executive operations." *Id.* It is true that the Supreme Court had discounted such concerns in the domestic security context, *see Keith*, 407 U.S. at 319-20, but as the Fourth Circuit explained, in dealing with hostile agents of foreign powers, the concerns are more compelling. More important, in the area of foreign intelligence, the expertise and constitutional powers of the Executive are paramount. As this Court has recognized, "for reasons of both constitutional authority and practical competence,

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

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

deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information." [REDACTED] Opinion and Order at 30 (footnote omitted); *see also Truong*, 629 F.2d at 914 ("Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.").

Executive practice also demonstrates a consistent understanding that the President has inherent constitutional authority, in accordance with the dictates of the Fourth Amendment, to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. *Cf. Youngstown Sheet & Tube Co.*, 343 U.S. 579, 610-11 (1952) (Frankfurter, J., concurring) (noting the importance, in constitutional analysis, of "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution"). Wiretaps for such purposes have been authorized by Presidents at least since the administration of President Roosevelt in 1940. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Before the passage of FISA in 1978, foreign intelligence wiretaps and searches were conducted without any judicial order pursuant to the President's inherent authority. *See, e.g., Truong*, 629 F.2d at 912-14; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000) ("Warrantless foreign intelligence collection has been an established practice of the Executive Branch for decades."). When FISA was first passed, moreover, it addressed solely electronic surveillance and made no provision for physical searches. *See Pub. L. No. 103-359*, § 807, 108 Stat. 3423, 3443-53 (1994) (adding provision for physical searches). As a result, after

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

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

a brief interlude during which applications for orders for physical searches were made to this Court despite the absence of any statutory procedure authorizing such applications, the Executive continued to conduct searches under its own inherent authority. Indeed, in 1981, the Reagan Administration, after filing an application with this Court for an order authorizing a physical search, filed a memorandum with the Court explaining that the Court had no jurisdiction to issue the requested order and explaining that the search could properly be conducted without a warrant pursuant to the President's inherent constitutional authority. See S. Rep. No. 97-280, at 14 (1981) ("The Department of Justice has long held the view that the President and, by delegation, the Attorney General have constitutional authority to approve warrantless physical searches directed against foreign powers or their agents for intelligence purposes.").

Thus, the Fourth Amendment does not require the Executive Branch to obtain a warrant prior to undertaking the electronic surveillance detailed in the attached Application. At least a significant purpose of the surveillance is to obtain foreign intelligence necessary to protect the United States from violent attack by [REDACTED]

[REDACTED] See National Security Certification. All that the Fourth Amendment requires is that the electronic surveillance be reasonable.

2. This Case Involves "Special Needs" Beyond the Normal Need for Law Enforcement

In addition, as noted by the Court of Review, the Supreme Court has repeatedly made clear that in situations involving "special needs" that go beyond a routine interest in general law enforcement, there are exceptions to the warrant requirement. See *In re Sealed Case*, 310 F.3d at 745-46; see also *Vernonia*, 515 U.S. at 653 (there are circumstances "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable") (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); see also *McArthur*,

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

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

531 U.S. at 330 ("We nonetheless have made it clear that there are exceptions to the warrant requirement. When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."). It is difficult to encapsulate in a nutshell the different circumstances the Court has found qualifying as "special needs" justifying warrantless searches. But generally when the Government faces an increased need to be able to react swiftly and flexibly, or when there are at stake interests in public safety beyond the interests in ordinary law enforcement, the Court has found the warrant requirement inapplicable. One important factor in determining whether the situation involves "special needs" is whether the Government is responding to an emergency beyond the need for general crime control. *See In re Sealed Case*, 310 F.3d at 745-46.

Thus, the Court has permitted warrantless searches to search property of students in public schools, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would "unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools"), to screen athletes and students involved in extra-curricular activities at public schools for drug use, *see Vernonia*, 515 U.S. at 654-655; *Earls*, 536 U.S. at 829-38, to conduct drug testing of railroad personnel involved in train accidents, *see Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 634 (1989), and to search probationers' homes, *see Griffin*, 483 U.S. 868. Many special needs doctrine and related cases have upheld *suspicionless* searches or seizures. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (implicitly relying on special needs doctrine to uphold use of automobile checkpoint to obtain information about recent hit-and-run accident); *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extra-curricular activities); *Michigan Dep't of State*

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

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

Police v. Sitz, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States v. Martinez-Fuerte*, 428 U.S. 543, 562 (1976) (road block near the border to check vehicles for illegal immigrants); *see also Chandler v. Miller*, 520 U.S. 305, 323 (1997) (noting that “where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as ‘reasonable’—for example, searches now routine at airports and at entrances to courts and other official buildings”); *cf. In re Sealed Case*, 310 F.3d at 746 (noting that suspicionless searches and seizures in one sense are a greater encroachment on privacy than electronic surveillance under FISA because they are not based on any particular suspicion, but “[o]n the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning”). To fall within the “special needs” exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary crime control. *See, e.g., Ferguson v. Charleston*, 532 U.S. 67 (2001) (hospital policy of conducting drug tests and turning over the results to law enforcement agents without the patients’ knowledge or consent does not fit within the “special needs” doctrine because the purpose served by the searches was indistinguishable from the general interest in crime control and law enforcement agents were extensively involved in implementing the policy); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000) (striking down use of roadblock to check for narcotics activity because its “primary purpose was to detect evidence of ordinary criminal wrongdoing”).

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the area of “special needs, beyond the normal need for law enforcement” where the Fourth Amendment’s touchstone of reasonableness can be satisfied without resort to a warrant. *Vernonia*, 515 U.S. at 653. Collecting foreign intelligence in time of armed conflict is far

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

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

removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like [REDACTED] including even the possibility of a foreign attack on the United States. As recognized by the Court of Review, "FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from 'ordinary crime control.' After the events of September 11, 2001 . . . it is hard to imagine greater emergencies facing Americans" 310 F.3d at 746; *cf. Edmond*, 531 U.S. at 44 ("the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack" because "[t]he exigencies created by th[at] scenario are far removed" from ordinary law enforcement); *Carroll v. United States*, 267 U.S. 132, 154 (1925) ("national self protection" reasonably supports border searches without probable cause or a warrant); *Cassidy v. Chertoff*, No. 05-1835-cv, slip op. at 22-23 (2d Cir. Nov. 29, 2006) ("It is clear to the Court that the prevention of terrorist attacks on large vessels engaged in mass transportation and determined by the Coast Guard to be at heightened risk of attack constitutes a 'special need.' Preventing or deterring large-scale terrorist attacks present[s] problems that are distinct from standard law enforcement needs and indeed go well beyond them."); *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006) ("preventing a terrorist from bombing the [New York] subways constitutes a special need that is distinct from ordinary post hoc criminal investigation"). In foreign intelligence investigations, moreover, the targets of surveillance include agents of foreign powers who may be specially trained in concealing their activities from our Government and whose activities may be particularly difficult to detect. The Executive requires a greater degree of

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

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

flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation.

In particular, the electronic surveillance detailed in the attached Application is designed to respond to the threat posed to our Nation's security by [REDACTED]

[REDACTED] "The nature of the 'emergency [caused by the events of September 11, 2001],' which is simply another word for threat, takes the matter out of the realm of ordinary crime control." *In re Sealed Case*, 310 F.3d at 746. The purpose of the Application is to enable the Government to react quickly and flexibly (and with secrecy) to new leads so that the Government may find agents of [REDACTED]

[REDACTED] in time to disrupt future terrorist attacks against the United States and its interests. Imposing the warrant and probable cause requirement that applies to ordinary criminal cases could prevent the Government from being able to exploit its advantages [REDACTED]

[REDACTED] As this Court has explained in a related case, "the Government's concern is to identify and track [REDACTED] and ultimately to thwart terrorist attacks. This concern clearly involves national security interests beyond the normal need for law enforcement and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion." [REDACTED]

[REDACTED] Opinion and Order at 51-52.

B. The Electronic Surveillance Detailed in the Application is Reasonable

The electronic surveillance described in the attached Application, which fully complies with FISA's requirements, is certainly reasonable. *Cf. In re Sealed Case*, 310 F.3d at 746

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

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

(expressing firm belief that "FISA as amended is constitutional because the surveillances it authorizes are reasonable"). As the Supreme Court has emphasized repeatedly, "[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)); *see also Earls*, 536 U.S. at 829 ("[W]e generally determine the reasonableness of a search by balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests."). The Supreme Court has found searches reasonable when, under the totality of the circumstances, the importance of the governmental interests outweighs the nature and quality of the intrusion on the individual's Fourth Amendment interests. *See, e.g., Samson v. California*, 126 S. Ct. 2193 (2006); *Knights*, 534 U.S. at 118-22. Under the standard balancing of interests analysis used for gauging reasonableness, the electronic surveillance described in the Application is consistent with the Fourth Amendment.

With respect to the individual privacy interests at stake, there can be no doubt that, as a general matter, interception of the content of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. *See Berger v. State of New York*, 388 U.S. 41, 56 (1967). The same privacy interest likely applies, absent individual circumstances lessening that interest, to the contents of e-mail communications. *See United*

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

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

States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (transmitter of an e-mail enjoys a reasonable expectation of privacy that the electronic communication will not be intercepted by a law enforcement officer without a warrant and probable cause, but once the communication is received by another person, the transmitter no longer enjoys the same expectation of privacy); cf. *Guest v. Leis*, 255 F.2d 325, 333 (6th Cir. 2001) (individuals lose a legitimate expectation of privacy in an e-mail that has already reached its recipient); 45 M.J. at 418-19 ("Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Messages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy."). As the U.S. Court of Appeals for the Second Circuit has recently held in two cases involving Government programs designed to prevent terrorist attacks on large vessels and the New York subway system, however, even where the individual expectation of privacy is undiminished, that interest may be outweighed by the Government's interest in protecting the Nation from terrorist attack. See *Cassidy*, slip op. at 14-15; *MacWade*, 460 F.3d at 272-23.

On the other side of the scale here, the Government's interest in conducting the surveillance is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack has already taken thousands of lives and placed the Nation in a state of armed conflict. Defending the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in the Constitution. See U.S. Const. art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion . . .") (emphasis added); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1862) ("If war be made by invasion of a foreign nation, the President is not

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

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

only authorized but bound to resist force by force . . ."). As the Supreme Court has declared, "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981); *see also Keith*, 407 U.S. at 312 ("unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered").

The Government's overwhelming interest in detecting and thwarting [REDACTED] attacks by [REDACTED] [REDACTED] is certainly sufficient to make reasonable the intrusion into privacy involved in targeting collection at communications with respect to which there is probable cause to believe that one communicant is a member or agent of [REDACTED] [REDACTED] and that one end is in a foreign country. The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days and that successfully struck at the command and control center for the Nation's military. As explained in the NCTC Declaration, [REDACTED]

[REDACTED]

NCTC Declaration ¶ 17; *see also id.* ¶ 155. It is the assessment of the Intelligence Community that [REDACTED]

[REDACTED]



[REDACTED]

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

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

and b(7)(E)



We recognize that, because the magnitude of the Government's interest here depends in part upon the threat posed by   the weight that interest carries in the balance may change over time. It is thus significant for the reasonableness of the surveillance detailed in the Application that the Court's authorization would be limited to a 90-day period, subject to Court-approved 90-day extensions. *See* 50 U.S.C. § 1805(e)(1). The Government expects to apply for regular 90-day extensions of the Court's order, *see id.* § 1805(e)(2). These applications will give the Government the opportunity to provide the Court with the latest

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

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

assessment of the threat posed by these foreign powers, thereby enabling the Court to evaluate whether that threat remains sufficiently strong that the Government's interest in protecting the Nation and its citizens from foreign attack continues to outweigh the individual privacy interests at stake.

In evaluating Fourth Amendment reasonableness, it is also significant that communications would be targeted for collection only if there is probable cause to believe that (1) one of the parties to the communication is a member or agent of [REDACTED] [REDACTED] and (2) that the communication is to or from a foreign country. The interception is thus targeted precisely at communications for which there is already a reasonable basis to think there is a connection to international terrorism. This is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia*, 515 U.S. at 663; *see also Earls*, 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). This does not mean, of course, that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. *See* [REDACTED] Opinion and Order at 52-53. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth

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

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

Amendment.”). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented—that is, some measure of fit between the search and the desired objective—is relevant to the reasonableness analysis.

The Supreme Court has repeatedly held that evaluating reasonableness under the Fourth Amendment depends on the totality of the circumstances, and thus no one factor is determinative. The electronic surveillance detailed in the Application, which would be carefully designed to collect only a limited number of communications in order to prevent a future catastrophic terrorist attack on our Nation, and which would be constrained by extensive Executive Branch oversight, would be reasonable even without judicial involvement. *Cf. Truong*, 629 F.2d 908, 916-17 (finding that, even in peacetime, a search for foreign intelligence purposes carried out without judicial approval was reasonable under the Fourth Amendment); *Butenko*, 494 F.2d 593, 606 (same). Here, however, the submission of the attached Application to this Court, and the fact that any order of this Court authorizing surveillance would be issued by a neutral, detached judge, add to the reasonableness of the surveillance. . *Cf. In re Sealed Case*, 310 F.3d at 742 (finding that FISA amplifies the President’s power in part because of the judicial role it allows). The Application has been filed by the Director of the NSA and approved by the Attorney General of the United States, and the Director of National Intelligence has certified that at least a significant purpose of the surveillance is to obtain foreign intelligence. In addition, the Application contains detailed minimization procedures to ensure that communications will be targeted for collection only if there is probable cause to believe that (1) one of the parties to the communication is a member or agent of [REDACTED]

[REDACTED]; and (2) that the communication is to or from a foreign country.

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

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

The minimization procedures also include several specific procedures that will be followed if a telephone number or e-mail address is reasonably believed to be used by a person in the United States. First, only three senior NSA officials will be authorized by the Director of the NSA to approve collection of communications linked to the targeted foreign powers, and all such approvals will be documented in writing. Second, a number or e-mail address used by a person in the United States may not be tasked for collection without the prior approval of the Attorney General, the Assistant Attorney General for the National Security Division (AAG/NSD), or the Deputy Assistant Attorney General in the National Security Division with responsibility for FISA operations and oversight (DAAG). Third, no such telephone number or e-mail address may be regarded as associated with [REDACTED] [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution. Fourth, the tasking of telephone numbers or e-mail addresses reasonably believed to be used by a person in the United States may not continue without the explicit approval of this Court. The Government will report to the Court twice a week on any new numbers or addresses that are reasonably believed to be used by persons in the United States. Included within each report will be a description of the basis for the determination by the NSA and the Attorney General, the AAG/NSD, or the DAAG that there was probable cause to believe that the number or address is associated with a member or agent of [REDACTED]

[REDACTED] If the Court does not approve any of the new telephone numbers or e-mail addresses within forty-eight hours of receiving the report, the Government would have twenty-four hours to submit additional information. If the Court does not, within twenty-four hours of receiving additional information from the Government, find that there is probable cause to

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

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

believe that any of the new numbers or addresses is associated with a member or agent of [REDACTED]
[REDACTED] the tasking of that
telephone number or e-mail address must cease and any acquired communications must be
segregated and may be retained only upon Court approval if the Government demonstrates a
foreign intelligence need for such retention. Finally, the NSA also will review telephone
numbers and e-mail addresses used by a person in the United States every 90 days to determine
whether tasking of the number or address should continue. *See* NSA Declaration ¶ 68.

Telephone numbers and e-mail addresses not reasonably believed to be used by a person
in the United States will be tasked only after an NSA analyst has documented in writing his
determination that the number or address meets the minimization probable cause standard and an
official in the NSA's [REDACTED] Branch has verified that
the analyst's determination has been properly documented. *Id.* ¶ 67. *Cf. United States v. Flores-*
Montano, 541 U.S. 149, 156 (2004) (Breyer, J., concurring) (noting that the "administrative
process [of keeping track of border searches] should help minimize concerns that gas tank
searches might be undertaken in an abusive manner"). In addition, an attorney from the National
Security Division at the Department of Justice will review the NSA's justifications for targeting
the numbers and addresses. Every thirty days, the Government will submit a report to the Court
listing new numbers and addresses that the NSA has tasked during the previous thirty days and
briefly summarizing the basis for the NSA's determination that there was probable cause to
believe that each number and address is associated with a member or agent of [REDACTED]

[REDACTED] At any time, the Court may request
additional information on particular telephone numbers or e-mail addresses and, if the Court
finds that there is not probable cause to believe that any number or e-mail address is associated

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

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

with a member or agent of [REDACTED]

[REDACTED] the Court may direct the collection of communications to and from that number or address to cease within forty-eight hours. The Court may also direct that any communications acquired using those particular numbers or addresses must be segregated and may be retained only upon Court approval if the Government demonstrates a foreign intelligence need for such retention.

In addition, with respect to the program as a whole, the NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate's Office of Oversight and Compliance will each periodically review this program. The Director of the NSA anticipates that, consistent with direction from the President, he will, in coordination with the Attorney General, inform the Congressional Intelligence Committees of the Court's approval of this collection activity if so granted. Finally, with every application to renew this authorization, the Government would explain its current understanding of which specific terrorist organizations are associated with [REDACTED]

[REDACTED]

In light of the considerations outlined above, taking into account the totality of the circumstances, including the nature of the privacy interest at stake, the overwhelming governmental interest involved, *i.e.*, [REDACTED]

[REDACTED]

[REDACTED] and the targeted nature of the surveillance at issue, the electronic surveillance detailed in the Application would be reasonable under the Fourth Amendment.

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

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

IV. The Application Fully Complies with the First Amendment

The proposed electronic surveillance is consistent with the First Amendment. Good faith law enforcement investigation and data-gathering activities using legitimate investigative techniques do not violate the First Amendment, at least where they do not violate the Fourth Amendment. See *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1064 (D.C. Cir. 1978). As Judge Wilkey has explained, "the First Amendment offers no procedural or substantive protection from *good faith* criminal investigation beyond that afforded by the Fourth and Fifth Amendments." *Id.* at 1057; see also *United States v. Gering*, 716 F.2d 615, 620 (9th Cir. 1983) (The use of mail covers, *i.e.*, the screening of the exterior of all mail addressed to an individual, does not violate the First Amendment if it is "otherwise permissible under the fourth amendment" and where there is no showing "that the mail covers were improperly used and burdened . . . associational rights."). But cf. *Reporters Comm.*, 593 F.2d at 1071 n.4 (Robinson, J.) (the other judge in the majority with Judge Wilkey) (the result of First Amendment analysis "may not always coincide with that attained by application of Fourth Amendment doctrine").

To be sure, interception of the contents of communications might in some cases implicate First Amendment interests, in particular freedom of speech and of association. See *Barnicki v. Vopper*, 532 U.S. 514, 532 (2001) ("[p]rivacy of communication is an important interest" protected by the First Amendment); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."). For example, in *Keith*, 407 U.S. at 314, the Supreme Court observed that "the fear of unauthorized official eavesdropping [might] deter vigorous citizen dissent and discussion of Government action in private conversation." But the concerns identified by the Court in *Keith* do not apply here.

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

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

Keith addressed a system of eavesdropping that targeted domestic organizations, and it did not consider the issues raised by surveillance aimed at foreign threats during an ongoing armed conflict. *See* 407 U.S. at 321 (“[T]his case involves only the domestic aspects of national security.”). Surveillance of domestic groups necessarily raises a First Amendment concern that generally is not present when the target of the surveillance is a foreign power. The Supreme Court explained in the domestic context that “[s]ecurity surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.” *Id.* at 320. As this Court has recognized, however, these concerns are not raised by surveillance “in furtherance of the compelling national interest of identifying and tracking [REDACTED] and ultimately of thwarting terrorist attacks. The overarching investigative effort against [REDACTED] is not aimed at curtailing First Amendment activities and satisfies the ‘good faith’ requirement.” [REDACTED] Opinion and Order at 68.

Although it might be argued that electronic surveillance could “chill” the exercise of First Amendment rights to speech and association, the Supreme Court has held that the “subjective ‘chill’” stemming from “the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose” does not constitute a cognizable injury. *Laird v. Tatum*, 408 U.S. 1, 10, 13 (1972). A perceived “chill” is not an injury under the First Amendment unless it is caused by an exercise of “regulatory, proscriptive, or compulsory” government power, or by a “specific present objective harm or a threat of specific future harm.” *Id.* at 11, 14; *see also Fifth Avenue Peace Parade Comm. v. Gray*, 480 F.2d 326, 332 (2d Cir. 1973) (FBI investigation of protestors, including an examination of bank records, did not violate

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

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

the First Amendment because the purpose of the investigation was "not to deter, not to crush constitutional liberties," but to prevent violence.). No such "objective harm" or "threat of specific future harm" is present here. On the contrary, the Government would be engaged in a legitimate investigation whose aim is to prevent international terrorism, not to suppress speech or to harass dissident organizations. Significantly, the success of the investigation requires that speech *not* be chilled; the only way for the Government to locate terrorist operatives is if they continue to communicate with each other using means which they believe—incorrectly—are free from the risk of detection.

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

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

CONCLUSION (U)

For the foregoing reasons, the Court should grant the requested Order. (U)

Respectfully submitted,

Dated: December 12, 2006

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*

(b)(6), (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//HUMINT//COMINT//NOFORN~~

~~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

[REDACTED]

(S)

Docket Number: b(7)(E)

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

[REDACTED]

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] 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]
[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]
[REDACTED]
[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

~~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]). 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]
[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]

FISA (TS)

Constitute “Facilities” Under

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)



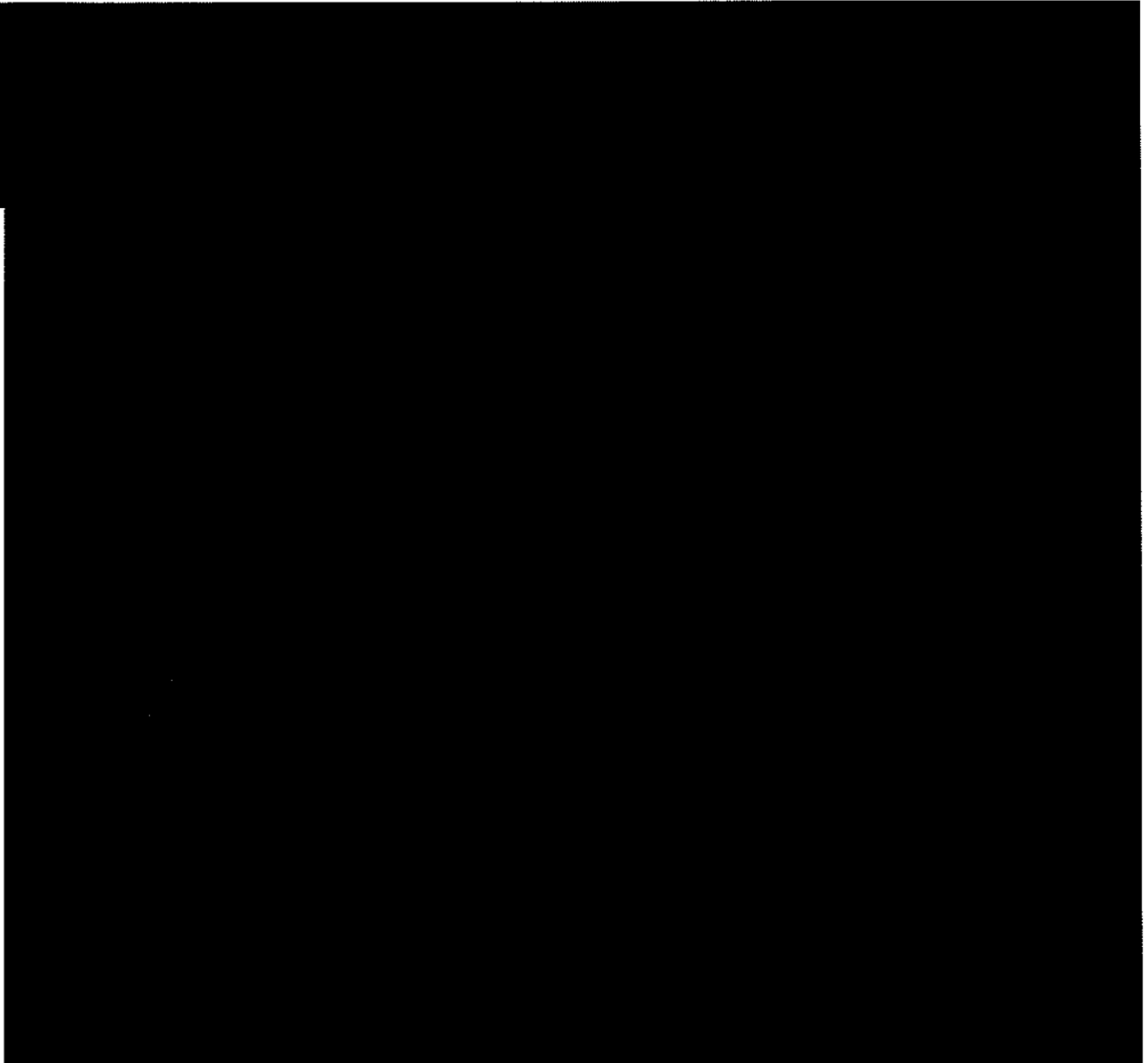
(TS//NF)

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)-

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

(S)-

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] 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] 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)

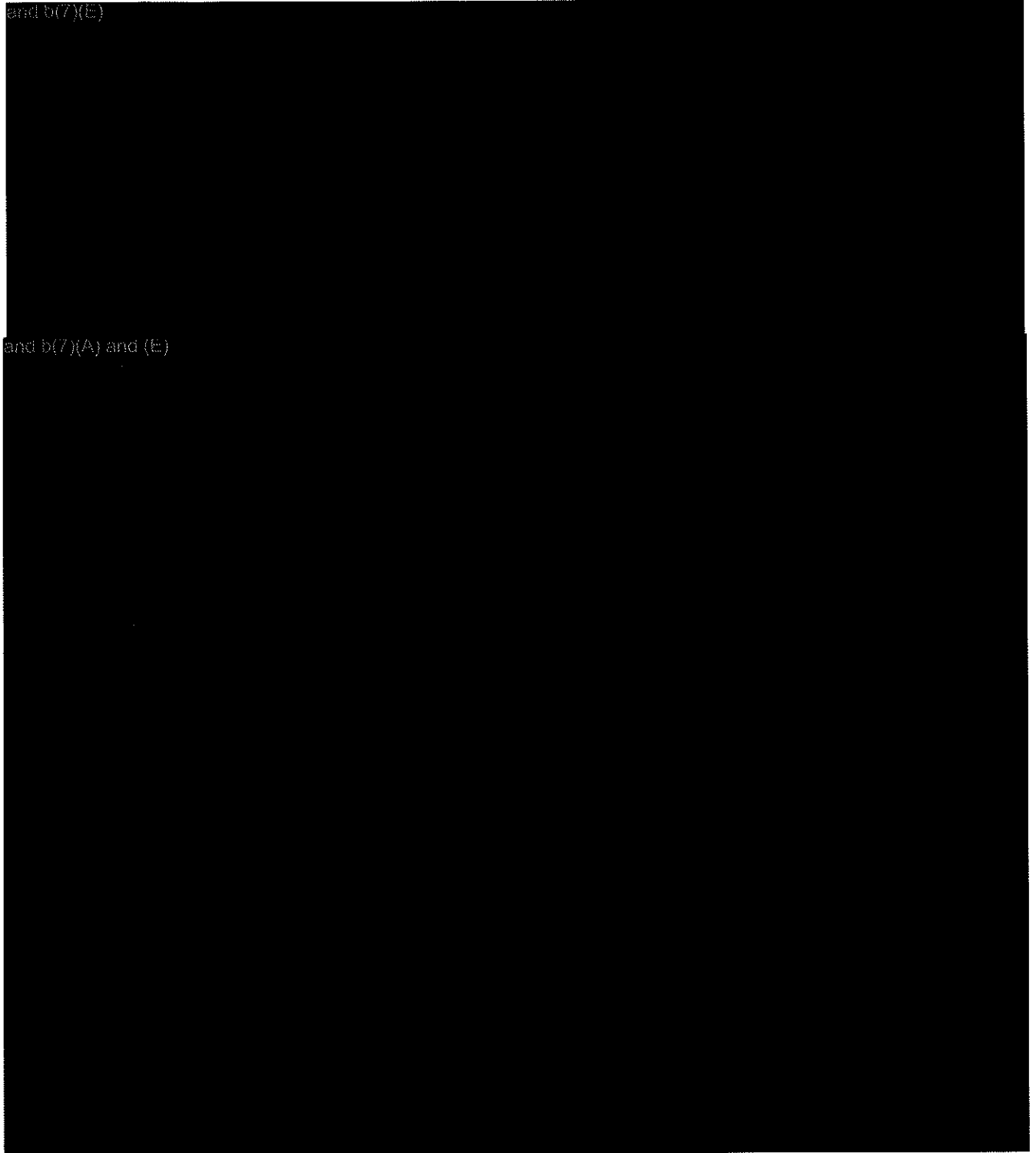
and b(6), b(7)(A), (C), and (E)



~~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.

~~(S)~~

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

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

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~~

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

~~THIS DECLARATION CONTAINS DESCRIPTIONS OF SENSITIVE INTELLIGENCE TECHNIQUES
AND PROPRIETARY INFORMATION; IT IS ONLY TO BE DISTRIBUTED TO PERSONNEL WITH A
SPECIFIC NEED TO KNOW~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE

Docket Number:

(S)

DECLARATION OF

NSA PROGRAM MANAGER FOR COUNTERTERRORISM SPECIAL PROJECTS

I, declare as follows:

1. ~~(TS//SI)~~ I am the Program Manager for NSA's Counterterrorism Special Projects. In that capacity, I am responsible to the Director of NSA for overseeing and integrating NSA's collection, processing and dissemination of foreign intelligence information from special source terrorist communications. I am also responsible for defining and implementing more effective means of

Derived From: NSA/CSSM 1-52

Dated: 20041123

Declassify On: 20310324

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

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

executing NSA's mission with respect to such communications, and for ensuring full compliance with all legal and policy requirements. [REDACTED]

[REDACTED]

[REDACTED] In addition to my current position, in the past I have held positions at NSA and/or in the intelligence community that required me to understand, among other things, the technical aspects of the collection of signals intelligence.

These prior positions include the following: (1) I helped design and implement NSA's

[REDACTED] (2) I developed the NSA collection, analysis and reporting response strategy following the [REDACTED] (3) I served as the lead analyst for the NSA response to the [REDACTED] and (4) I served as the Executive Assistant to the Deputy Director of Central Intelligence and later to the Director of Central Intelligence.

2. (FS//SI) I make this declaration in support of the Government's December 13, 2006, Application ("Government's Application") to conduct electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1862, as amended ("FISA"). As set forth in the Declaration of Lieutenant General Keith B. Alexander, Director of the National Security Agency ("NSA") (Exhibit C of the Government's Application) ("NSA Declaration"), the surveillance authority requested will enable NSA to target the communications of [REDACTED]

[REDACTED]

¹ (S//SI//NF//OC) For purposes of this Declaration, the phrase [REDACTED]

[REDACTED]

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

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

[REDACTED] in the United States and abroad. This authority also will enable NSA to disseminate relevant information to support the efforts of the United States, and in particular the FBI, to detect and prevent terrorist acts against the United States. NSA will accomplish this by targeting for collection communications where there are reasonable grounds to believe that one of the communicants is a member or agent of [REDACTED] [REDACTED] and also that the communication is to or from a foreign country. A significant purpose of the surveillance is to obtain foreign intelligence necessary to protect the United States from actual or potential

[REDACTED]

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

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

attacks, other grave hostile acts, sabotage, or international terrorism by [REDACTED]
[REDACTED]

3. (S//SI) This declaration is divided into three sections. First, it provides an overview of NSA's signals intelligence ("SIGINT") collection system. Second, it briefly describes the need for an agile and effective early warning surveillance system to counter the threat the targeted foreign powers pose to the United States. Finally, it explains why the proposed surveillance would establish under FISA a technologically feasible and effective early warning surveillance system. My statements in this declaration are based on my personal knowledge of SIGINT collection and NSA operations, my review of the Application, information available to me in my capacity as the [position/title], and the advice of counsel.

I. (U) Overview of the National Security Agency's SIGINT system

4. (U) The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. Under Executive Order 12333, § 1.12(b), as amended, NSA's cryptologic mission includes three functions: (1) to collect, process, and disseminate signals intelligence information for national foreign intelligence and counterintelligence purposes and the support of military operations; (2) to conduct information security activities; and (3) to conduct operations security training for the U.S. Government.

5. (S) NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities as set forth in Executive Order No. 12333. In performing its SIGINT mission, NSA has developed a sophisticated worldwide SIGINT collection

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

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

network that acquires, among other things, foreign and international electronic communications and related information.

6. (S) NSA's collection and analysis of SIGINT for foreign intelligence purposes serves two primary goals. The first and most important goal is to gain as much information as possible in order to allow the United States to counter threats to the nation's security. The second goal is to obtain information critical to the formulation of U.S. foreign policy. Foreign intelligence information provided by NSA is relevant to a wide range of important issues, including international terrorism, threat warnings and readiness, military order of battle, arms proliferation, and foreign aspects of international narcotics trafficking.

7. (S) NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by SIGINT activities is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other means.

8. (S//SI) While signals intelligence produces critical foreign intelligence information, collecting this intelligence poses a formidable and constantly evolving challenge. The sheer volume and variety of electronic communications, and the rapid pace of technological change, make the effective collection of SIGINT exceedingly difficult. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

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

[REDACTED]

9. (TS//SI//NF//OC) The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and an incalculable expenditure of human effort. NSA's SIGINT collection network relies on a diverse and sophisticated suite of collection and processing technologies. Examples of the communications NSA intercepts around the globe include:

[REDACTED]

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

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

II. (U) The Government's Proposed Surveillance

10. (TS//SI) The Government's Application to this Court seeks authorization to conduct surveillance that will serve as part of NSA's signals intelligence system. The proposed surveillance would establish a critical component of an early warning system under FISA designed to alert the U.S. Government to the presence and intentions of members and agents of [REDACTED]

11. (S) The foreign powers targeted in this Application— [REDACTED]

[REDACTED] pose the greatest threats to the United States. Declaration of John S. Redd, Director of the National Counterterrorism Center (Exhibit B of the Government's Application) ("NCTC Declaration") at ¶¶ 155-157.

12. (TS//SI) The Intelligence Community believes that the United States must continue to use every collection tool available to prevent future attacks by [REDACTED] international terrorist groups. Id. at ¶ 157. The NCTC Declaration makes it clear that [REDACTED] intend to undertake future terrorist attacks and to continue to develop their existing capabilities in order to execute a potentially catastrophic attack in the United States. Id. at ¶ 17. It

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

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

describes in detail the tactics and techniques [REDACTED] employs in seeking to carry out such attacks.

Id. at ¶¶ 17-27.

13. (TS//SI//NF) [REDACTED] the NCTC Declaration states that the U.S. Government regards

[REDACTED] highest concern. Id. at ¶ 102. The Intelligence Community regards [REDACTED]

[REDACTED] Id. at ¶ 96. The NCTC Declaration notes that

intelligence reporting continues to yield examples of potential [REDACTED] contingency planning for

future attacks on U.S. interests, [REDACTED] Id. at ¶ 103.

14. (TS//SI//NF) In addition, the foreign powers targeted in the Government's Application

[REDACTED] make extensive use of modern telecommunications networks, including the Internet. [REDACTED]

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

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

15. (TS//SI)

16. (TS//SI//NF)

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

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

[REDACTED]

17. (TS//SI) The combination of the urgent threat to the United States posed by these foreign powers and the techniques they employ to evade detection by the U.S. Government underscores the need for an agile and efficient early warning system designed to detect their activities as quickly as possible. [REDACTED]

[REDACTED] present critical challenges for the nation's communications intelligence capabilities. NSA's SIGINT system is essential to our ability to identify the enemy and to detect and disrupt its plans for further attacks on the United States. Signals intelligence often is the only means the United States has to learn the identities of particular individuals who are involved in terrorist activities and the existence of particular terrorist threats.

18. (TS//SI//NF//OC) Accordingly, as detailed in the Government's Application, the "facilities" at which the electronic surveillance would be directed are: for telephone calls,

[REDACTED]
[REDACTED] and for e-mails,³ [REDACTED]

19. (TS//SI//NF//OC) NSA has reasonable grounds to believe that [REDACTED] e-mail

³ (TS//SI) The Government uses the term "e-mail" herein to refer to [REDACTED]
[REDACTED] As described in the NSA Director's Declaration at Exhibit C of the Government's Application, NSA will target for collection such electronic communications by [REDACTED]
[REDACTED]

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

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

addresses and telephone numbers are being used by agents or members of these foreign powers. Moreover, both the agents and members of these groups, and the telephone numbers and e-mail addresses from which they are communicating, are changing constantly. As a result, each month NSA likely will add to this list between [REDACTED] additional telephone numbers and e-mail addresses used by the targets, as well as remove other numbers and addresses. The majority of these new addresses will be foreign e-mail addresses.

III. (U) The Proposed Surveillance Would Establish a Technologically Feasible and Effective Means for Collecting Vital Intelligence that Would Otherwise Be Lost

20. (TS//SI//NF//OC) The proposed surveillance set forth in the Government's Application would provide for a technologically feasible and effective means of establishing an early warning surveillance system under FISA. [REDACTED]

[REDACTED]

[REDACTED] As described in detail below, the advantages of the proposed surveillance are (1) increased speed and agility in the collection of intelligence; and (2) with respect to e-mail, the ability to obtain additional, crucial information about suspected terrorists that we have not obtained under the customary approach of collecting only communications to and

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

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

from specific e-mail addresses.

A. (C) Increased Speed and Agility

21. (TS//NF//OC) First, the proposed surveillance would allow NSA to collect intelligence with greater speed and agility than would be possible by filing individual FISA applications or requests for emergency approval. The Government's ability to move quickly to intercept communications is critical to the effective operation of an early warning system. When the Government obtains information suggesting there are reasonable grounds to believe that a particular telephone number or e-mail address is being used by a terrorist operative, it must move as expeditiously as possible to initiate surveillance. To be effective, NSA must be able to employ its early warning surveillance capabilities to [REDACTED]

[REDACTED]

22. (TS//SI) Under the proposed surveillance system, trained NSA intelligence analysts would make targeting decisions after determining and properly documenting that the minimization probable cause standard is met – that is, there are reasonable grounds to believe that one of the communicants is an agent or member of one of the targeted foreign powers and that the communication is to or from a foreign country. In the case of a telephone number or e-mail address that is reasonably believed to be used by a person outside the United States, [REDACTED]

[REDACTED]

[REDACTED] in the case of a telephone number that is reasonably

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

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

believed to be used by a person inside the United States, for which NSA would be required to obtain the approval of a high-ranking Department of Justice official prior to initiating surveillance, NSA would still be able to begin receiving communications [REDACTED] of identifying a new telephone number.

23. (TS//SI//NF) The more typical approach of filing individual applications directed at specific e-mail addresses and telephone numbers used by terrorists cannot operate with the speed and agility needed to accomplish the objectives of the proposed surveillance and necessarily does not implement the critical early warning capability that is the purpose of the surveillance proposed in the Government's Application. [REDACTED]

[REDACTED]

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

[REDACTED]

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

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

[REDACTED]

In addition, each month NSA likely will add to this list between [REDACTED] additional telephone numbers and e-mail addresses used by the targets. At the same time, it also routinely will remove numerous such telephone numbers and e-mail addresses from this list. 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 under the customary framework of directing surveillance at specific telephone numbers and e-mail addresses. Any attempt by NSA to meet the demands of such an increase in individual FISA submissions would likely have severe impact on its operational effectiveness.

25. (TS//SI//NF) As described above, terrorists are adept at exploiting the features of the global communications system, particularly the Internet, to evade detection through a variety of means. [REDACTED]

[REDACTED]

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

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

[REDACTED]

[REDACTED]

[REDACTED] Thus, in certain cases, seeking emergency authorization before initiating collection on a newly identified e-mail address or telephone number will inevitably result in the loss of valuable intelligence, even given efficient processing of applications.

26. (S//SI) In short, compared to the more common approach under FISA of filing individual applications directed at facilities that are specific telephone numbers and e-mail addresses, the Government's proposed surveillance provides the necessary speed and agility to follow up quickly on new leads and to allow the Government to obtain actionable intelligence information that otherwise might be lost or obtained too late. It is always advantageous to collect signals intelligence as quickly as possible. Thus, one of the most important features of the proposed early warning surveillance is the ability to move as quickly as possible to conduct surveillance on the communications of suspected terrorists.

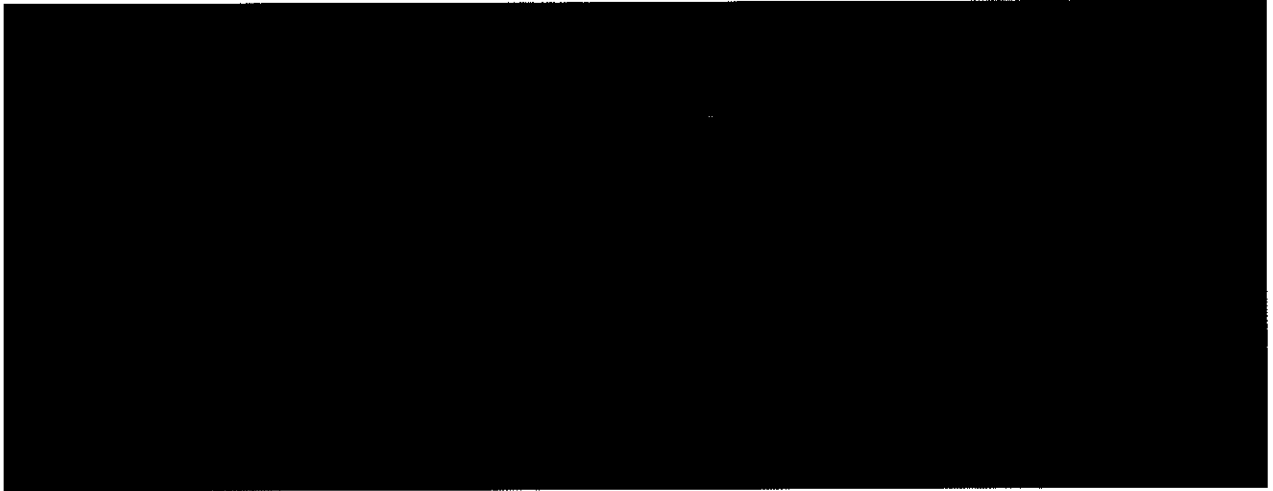
B. (U) Collection of Additional Foreign Intelligence

27. (TS//SI//NF//OC) In addition to providing for the speed and agility that is essential to an effective early warning system, the proposed surveillance would enable NSA to collect other forms of critical foreign intelligence that it could not obtain under the more customary framework of directing surveillance at specified e-mail addresses and collecting only communications to and from them. [REDACTED]

[REDACTED]

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

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



28. (TS//SI) First, under the proposed surveillance, NSA would collect electronic communications that contain the targeted e-mail address in the substantive contents of a communication between two third parties. Thus, even when an e-mail is not to or from the targeted e-mail address, NSA would collect the communication as long as the contents of the communication contained the e-mail address. For example, if an unknown [REDACTED] passes a targeted address to another unknown terrorist, NSA would collect that e-mail. [REDACTED]



29. (TS//SI) [REDACTED]



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

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

[REDACTED]

30. (TS//SI)

[REDACTED]

[REDACTED]

31 (TS//SI)

[REDACTED]

[REDACTED]

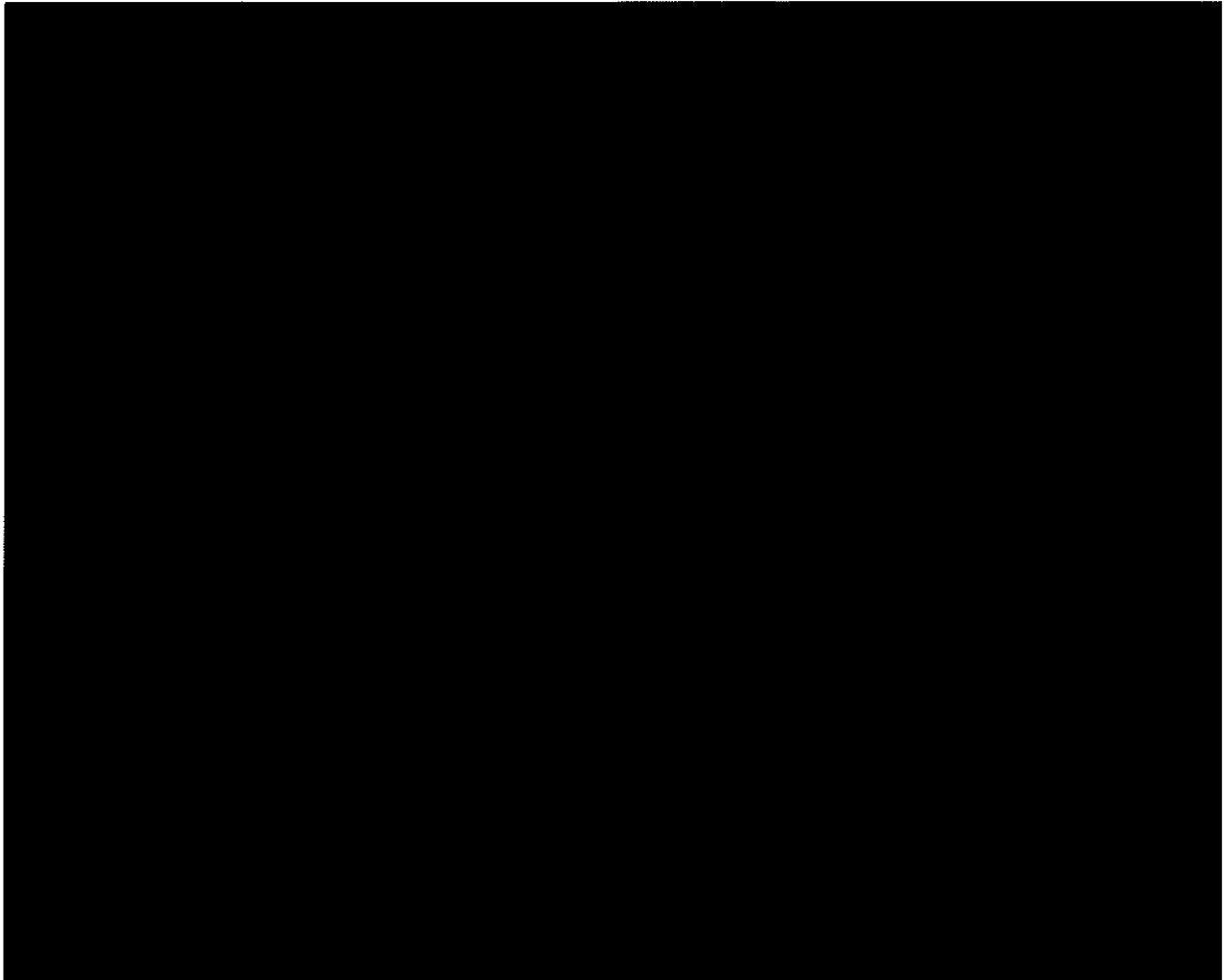
32. (TS//SI)


[REDACTED]

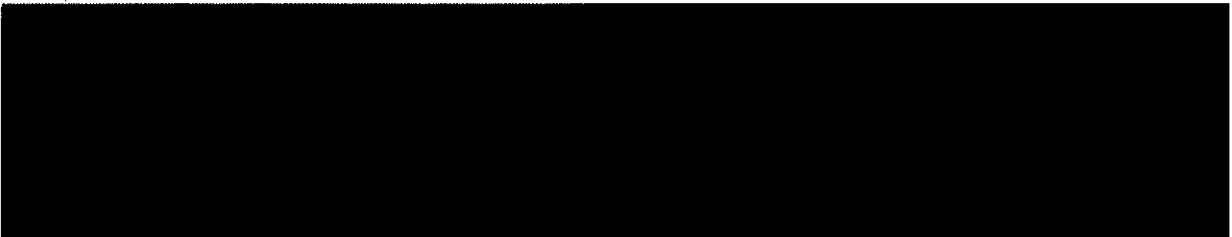
[REDACTED]

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

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



33. (TS//SI) Under the proposed method of conducting electronic surveillance, then, NSA will be in a position not only to learn information about the activities of its targets, but also to discover information about new potential targets that it may never have otherwise acquired. 



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

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

IV. (U) Conclusion

34. For all these reasons, [REDACTED]

[REDACTED]

The proposed surveillance set forth in the Government's Application will allow NSA to establish under FISA an early warning system to detect and prevent terrorist activities by the targeted foreign powers.

I declare under penalty of perjury that the foregoing is true and correct.

Signed this _____ day of _____, 2007.

b(3), b(6), and
NSA Program Manager
Counterterrorism Special Project

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

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

CLERK

2007

U.S. Foreign Intelligence
Surveillance Court

IN RE

:

: Docket Number:

b(7)(E)

:

(S):

ORDER

The United States of America has applied, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 ("FISA" or "the Act"), for an order for electronic surveillance to target for collection communications for which there is probable cause to believe: (1) that one of the communicants is a member or agent of

and (2) that the communication is to or from a foreign country.

The Court has given full consideration to the matters set forth in the Government's application 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)];

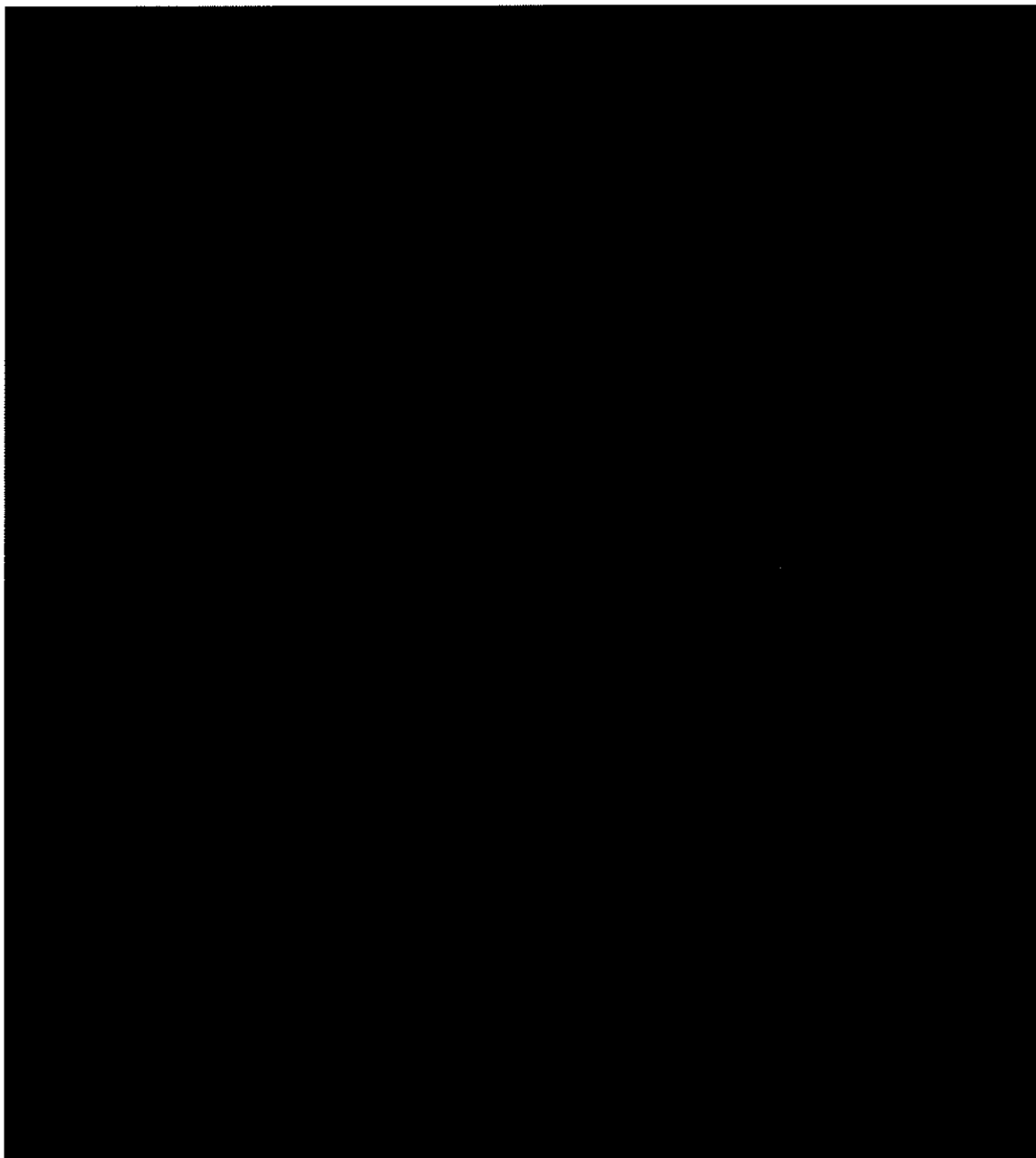
Derived from: Application to the USFISC in

b(7)(E)

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

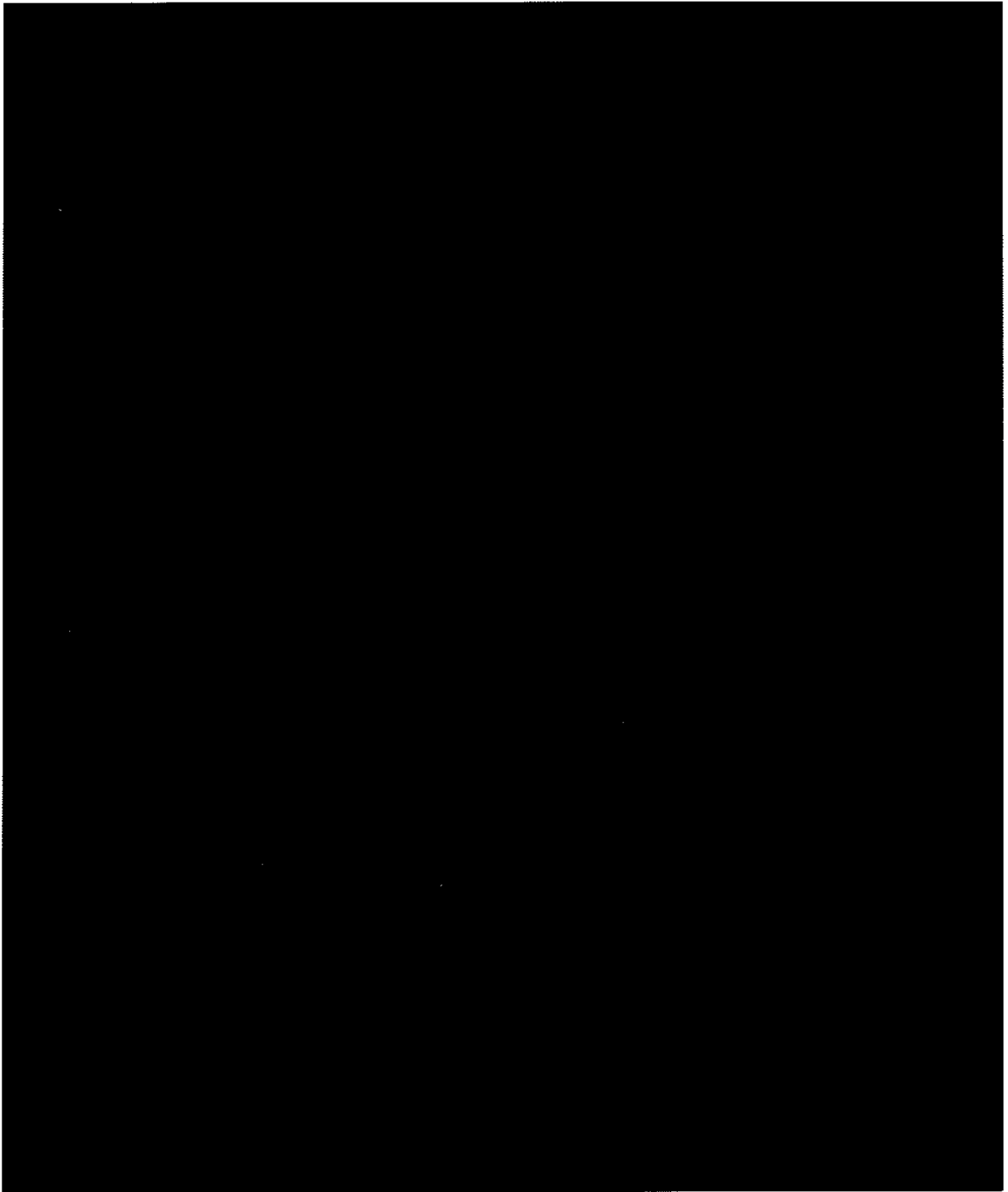
~~TOP SECRET//COMINT//NOFORN~~

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~~

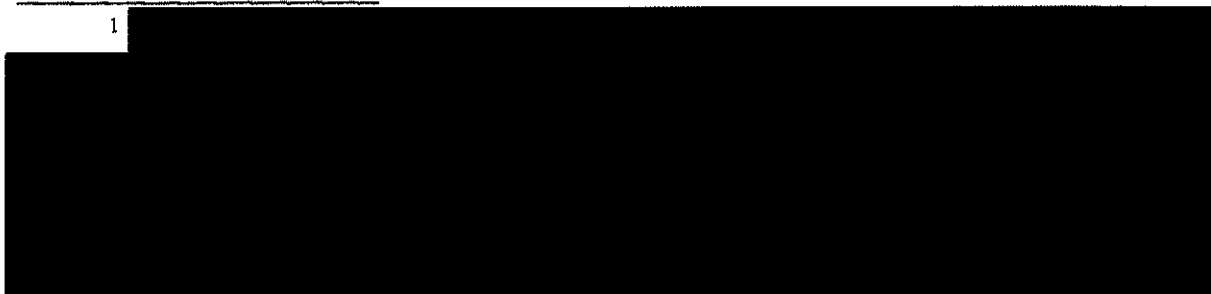


~~TOP SECRET//COMINT//NOFORN~~

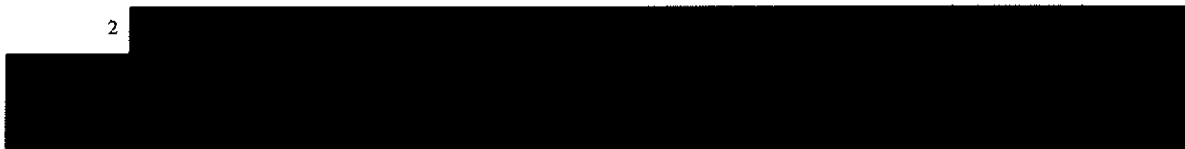
~~TOP SECRET//COMINT//NOFORN~~



1




2



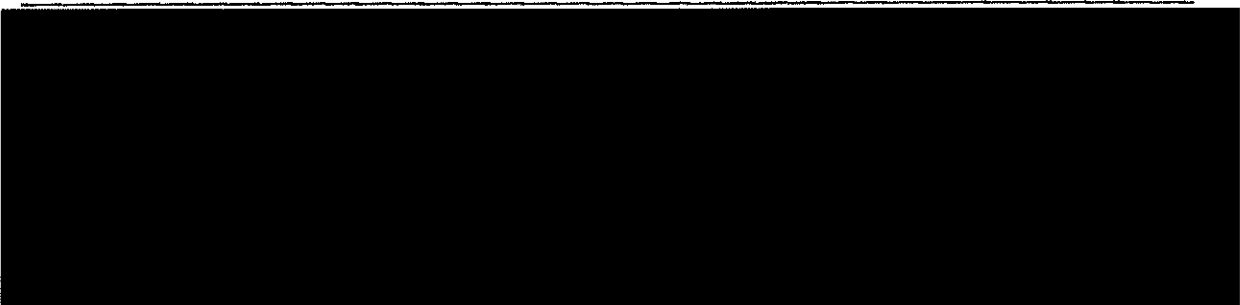
~~TOP SECRET//COMINT//NOFORN~~

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

(c) each of the facilities ³ 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 C to the application [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 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)].



³ 

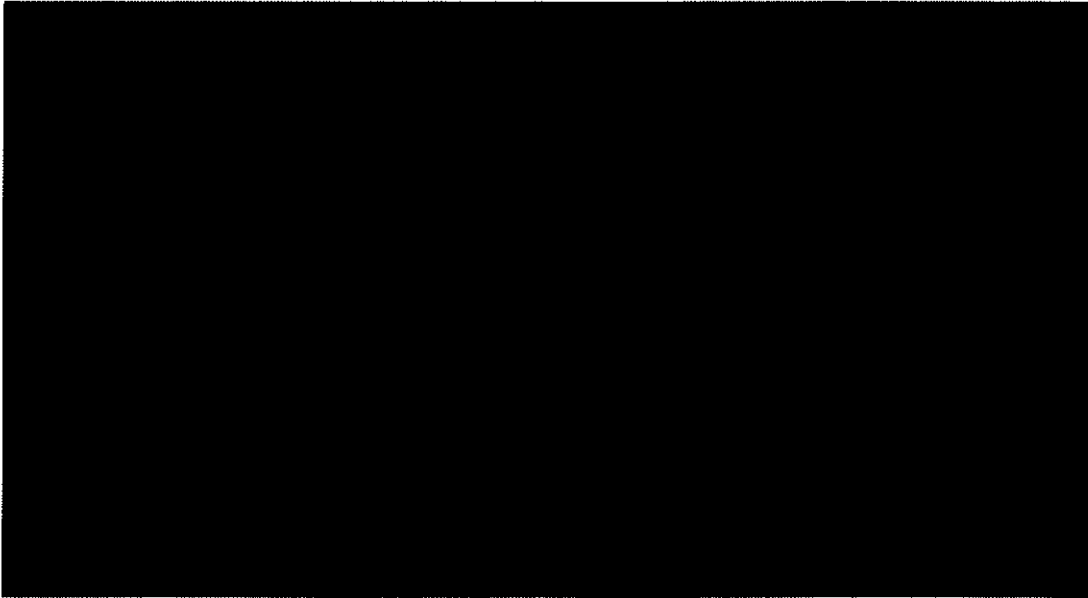

~~TOP SECRET//COMINT//NOFORN~~

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

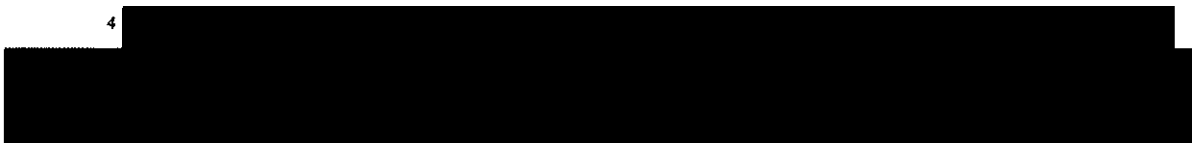
WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States to conduct electronic surveillance, as described in the application, is GRANTED as modified herein, and it is

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

(1) The United States is authorized 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, for a period of **ninety days**, unless otherwise ordered by the Court, as follows:

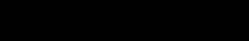


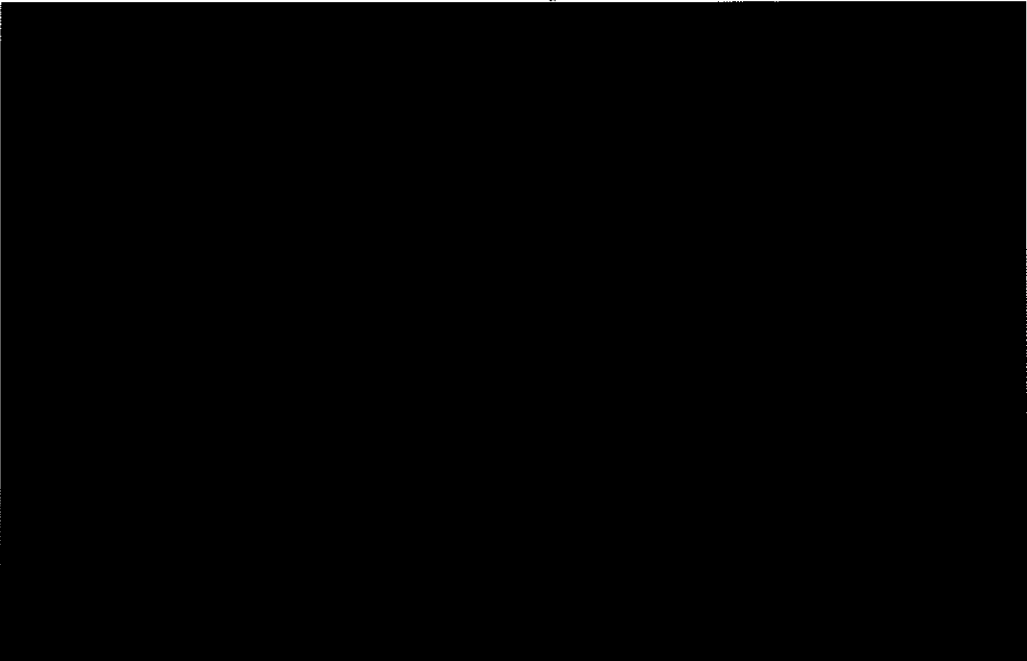
4



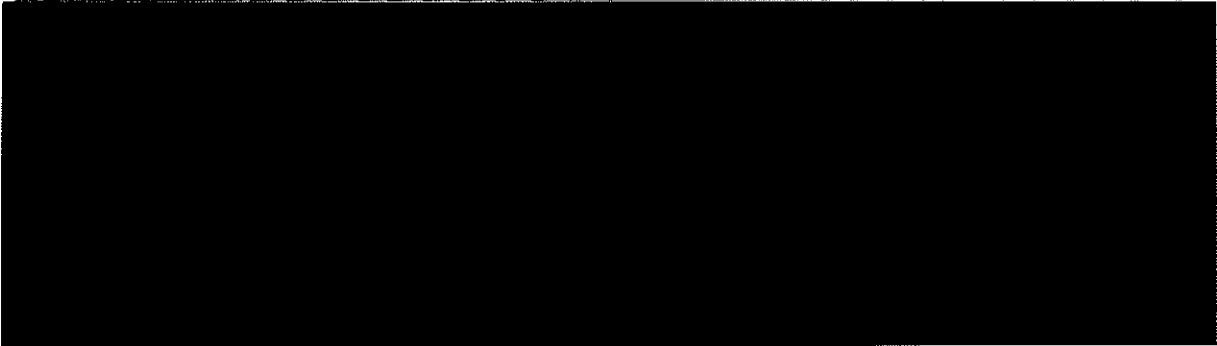
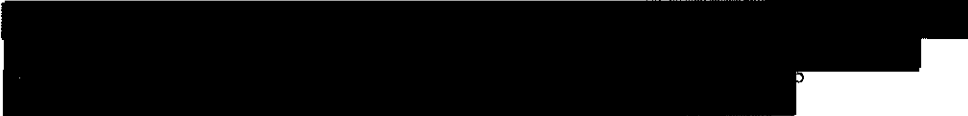
~~TOP SECRET//COMINT//NOFORN~~

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

 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



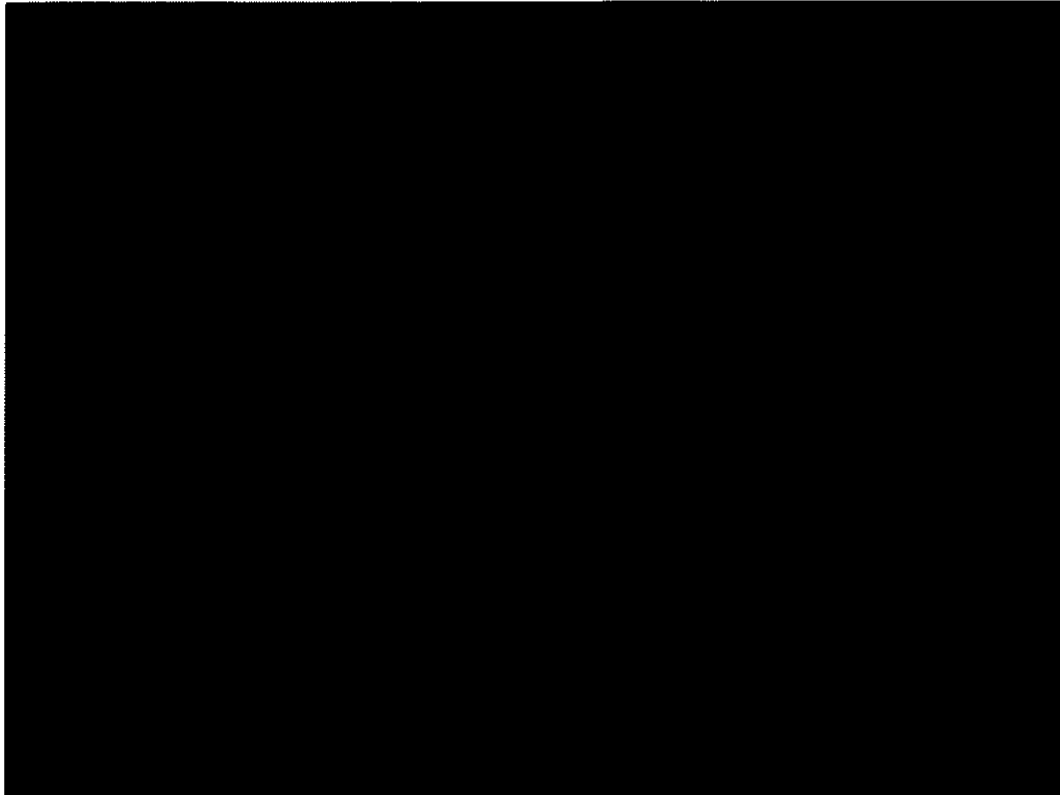
NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA



⁵ 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

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

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



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.

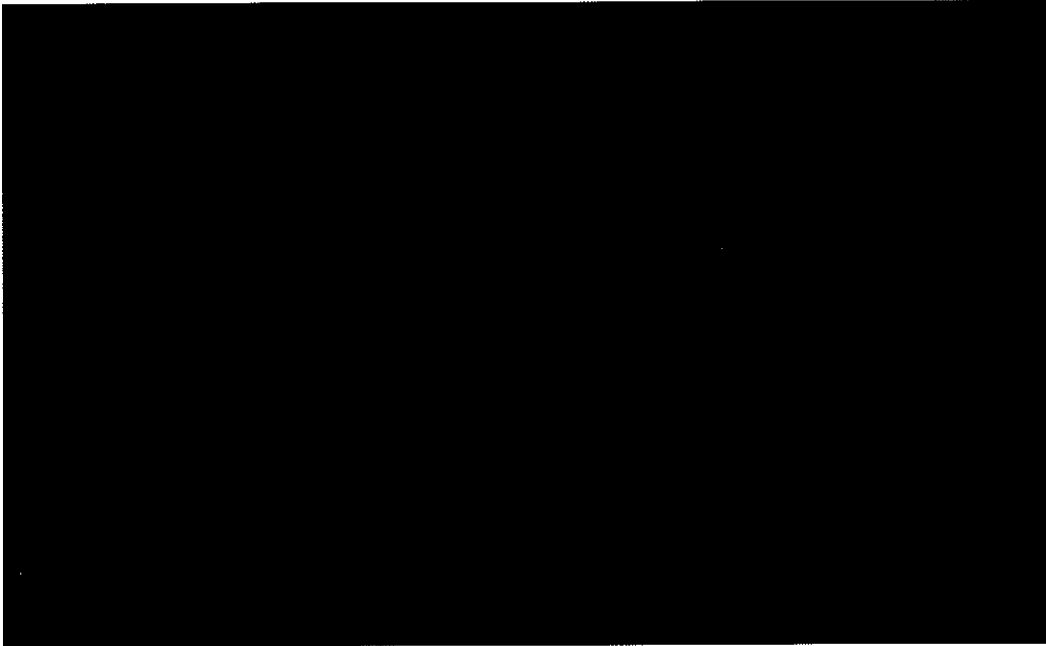
⁶ The Court understands that the system will select for delivery to NSA not only international Internet communications to and from agents or members of [REDACTED]

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

⁷ [REDACTED]

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

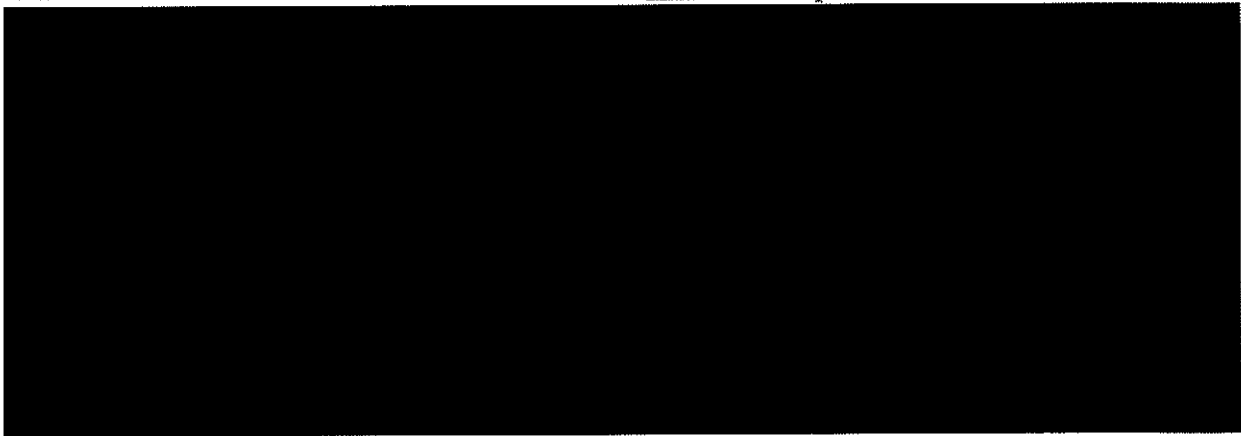
~~TOP SECRET//COMINT//NOFORN~~



8

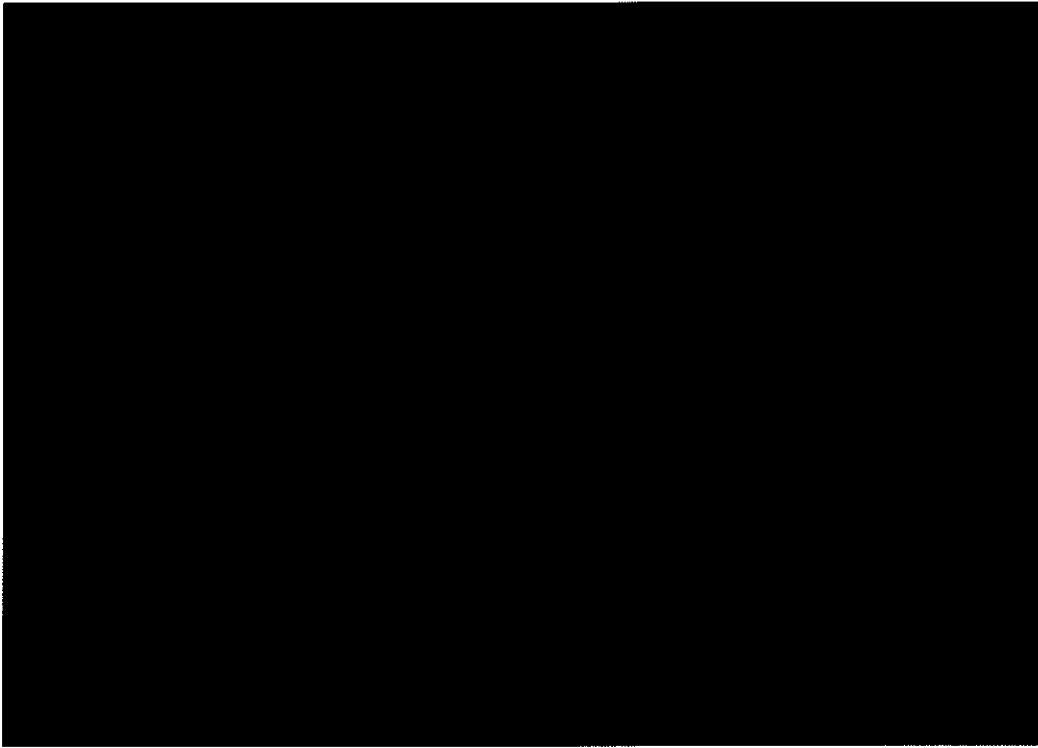


⁹ The Court understands that "selectors" as used herein to discuss the collection of Internet communications refers to e-mail addresses. [REDACTED]

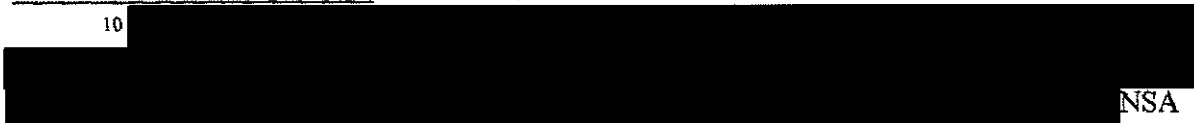


~~TOP SECRET//COMINT//NOFORN~~

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



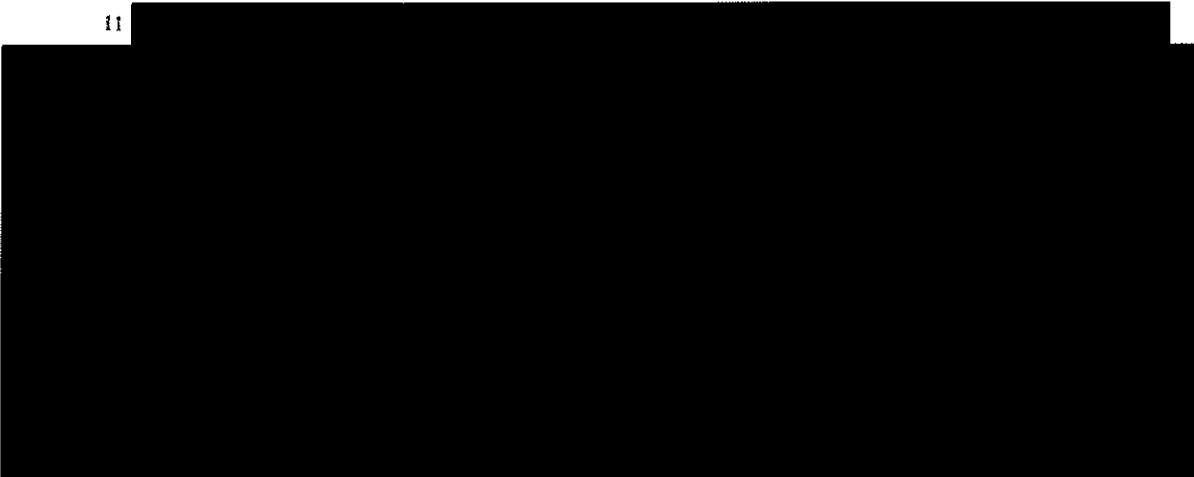
10



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.

11

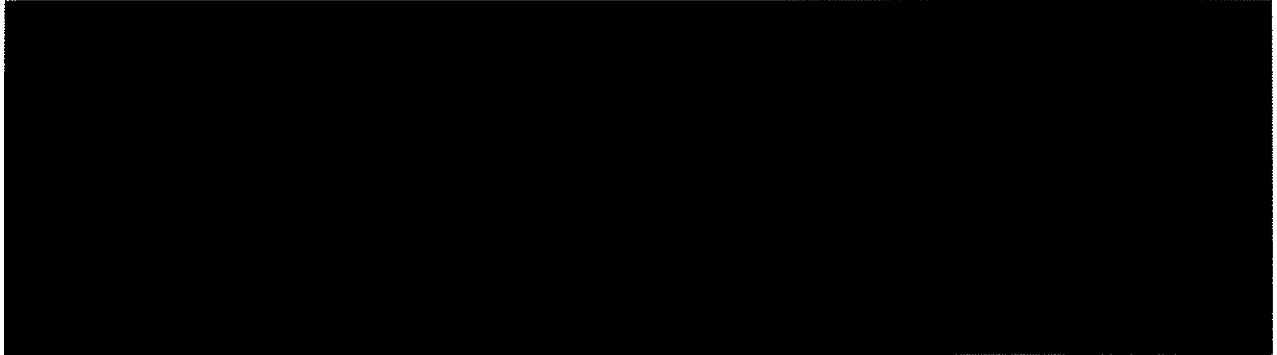


~~TOP SECRET//COMINT//NOFORN~~

~~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:



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)].

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

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

(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]

[REDACTED]

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.¹²

¹² 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~~

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 [REDACTED]

[REDACTED] to the application 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 reasons for such a belief. [REDACTED] as

described in Exhibit C to the application. The proposed number or e-mail address and supporting documentation shall be reviewed by officials from the [REDACTED]

[REDACTED] Branch within NSA.¹³ 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

¹³ 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~~

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 program to ensure it is being carried out lawfully, and shall submit an initial report to the Director of NSA sixty (60) days after the initiation of collection to assess the adequacy of the management controls and to assure that the processing and dissemination of U.S. person information is being accomplished in accordance with the minimization procedures specified herein.

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]
[REDACTED] the Court may direct that surveillance under this Order shall cease on that selector

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

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

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;

(b) [REDACTED]

[REDACTED]

[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

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

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

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;

(b) Certain of the modifications to the standard NSA FISA minimization procedures for electronic surveillance adopted by this Court in *In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets*, Order, No. ⁺(7)(E) (May 10, 2002) ("*Raw Take Motion*"), which modifications are set forth below:

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

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

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

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:¹⁴

(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.

¹⁴ and b(7)(E)

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

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

(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.

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 C to the application.

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

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

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.

(5) With each request for reauthorization, the Government shall (i) present a list of current selectors previously reported to the Court that the Government intends to continue to task for collection under the reauthorization; (ii) identify any such selectors that are reasonably believed to be used by U.S. persons outside the United States; and (iii) assess the efficacy of the surveillance described in footnote 6 above in acquiring the communications of the targeted foreign powers.

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

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

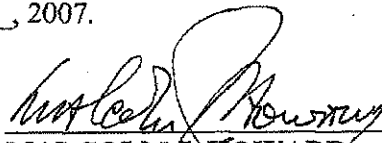
(6) The CIA shall minimize all communications received under this order as provided in Exhibit F to the application.

Signed 01-10-2007 002:18 Eastern Time
Date Time

This authorization regarding [REDACTED]

[REDACTED] expires at 3:00 pm

on the 6th day of APRIL, 2007.


MALCOLM J. HOWARD
Judge, United States Foreign
Intelligence Surveillance Court

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

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

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE VARIOUS KNOWN AND UNKNOWN :

AGENTS OF [REDACTED] :

: Docket Number: b(7)

PRESUMED UNITED STATES PERSONS (S) :

ORDER

The United States of America having applied, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 ("FISA" or "the Act"), for an order for electronic surveillance targeting **Various Known and Unknown Agents of** [REDACTED] [REDACTED] presumed U.S. persons, and the Court, having given full consideration to the matters set forth in the Government's application, 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 b(7)(E)

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

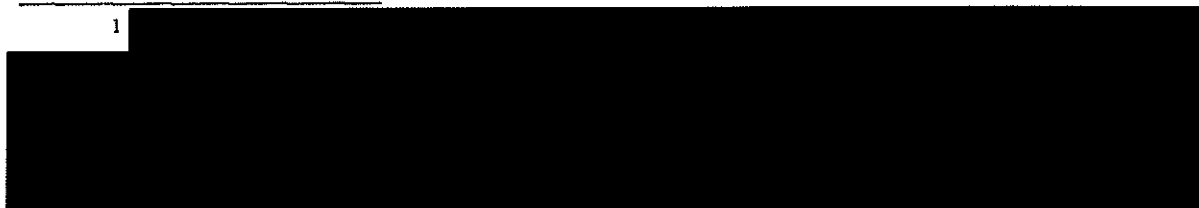
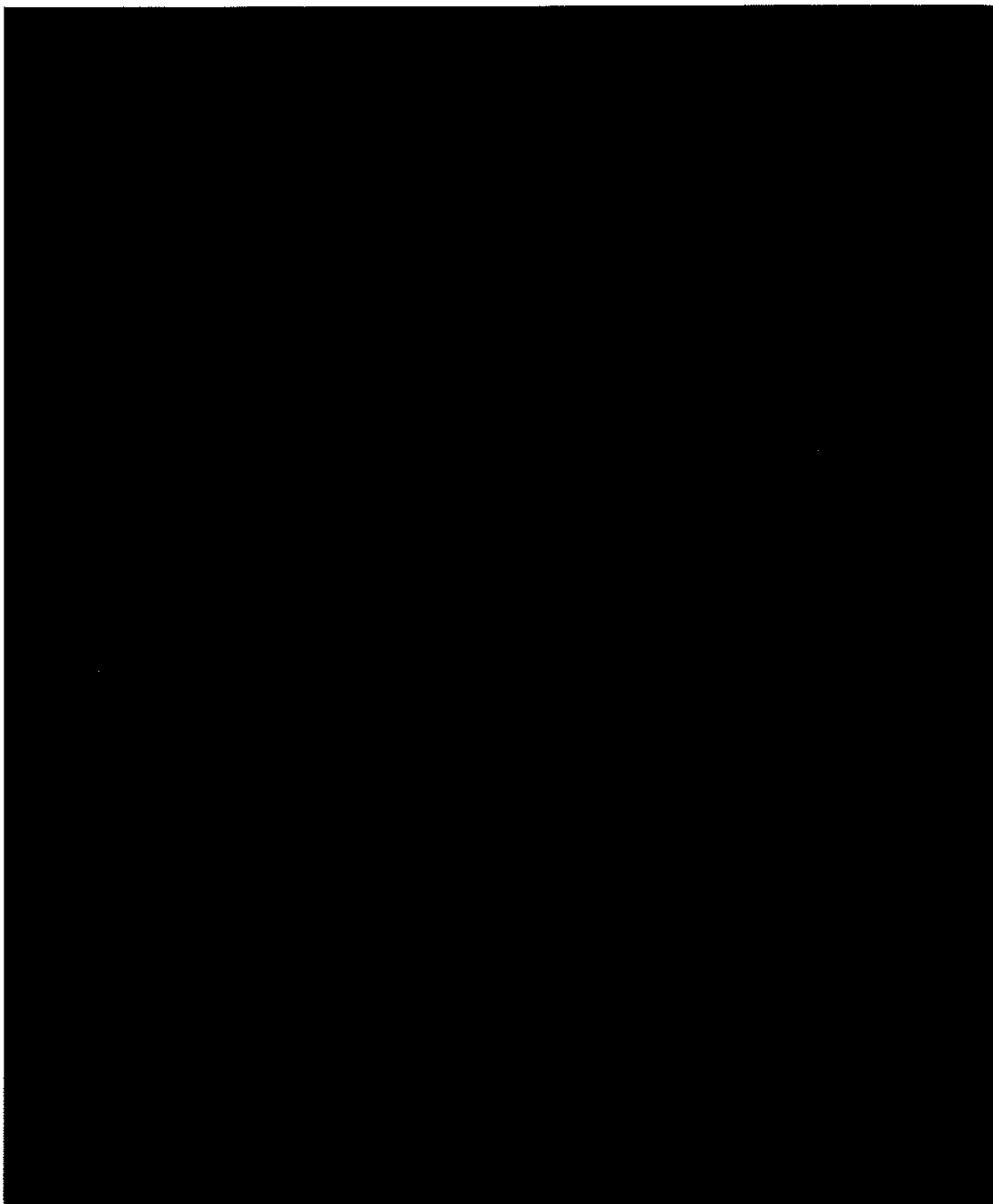
3. On the basis of the facts submitted by the applicant, there is probable cause to believe that [50 U.S.C. § 1805(a)(3)]:

(a) [REDACTED] as further referenced in Exhibit B, together, constitute a group engaged in international terrorism or activities in preparation therefor, and, therefore, is a foreign power as defined by 50 U.S.C. § 1801(a)(4):

[REDACTED]

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

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



1

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

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

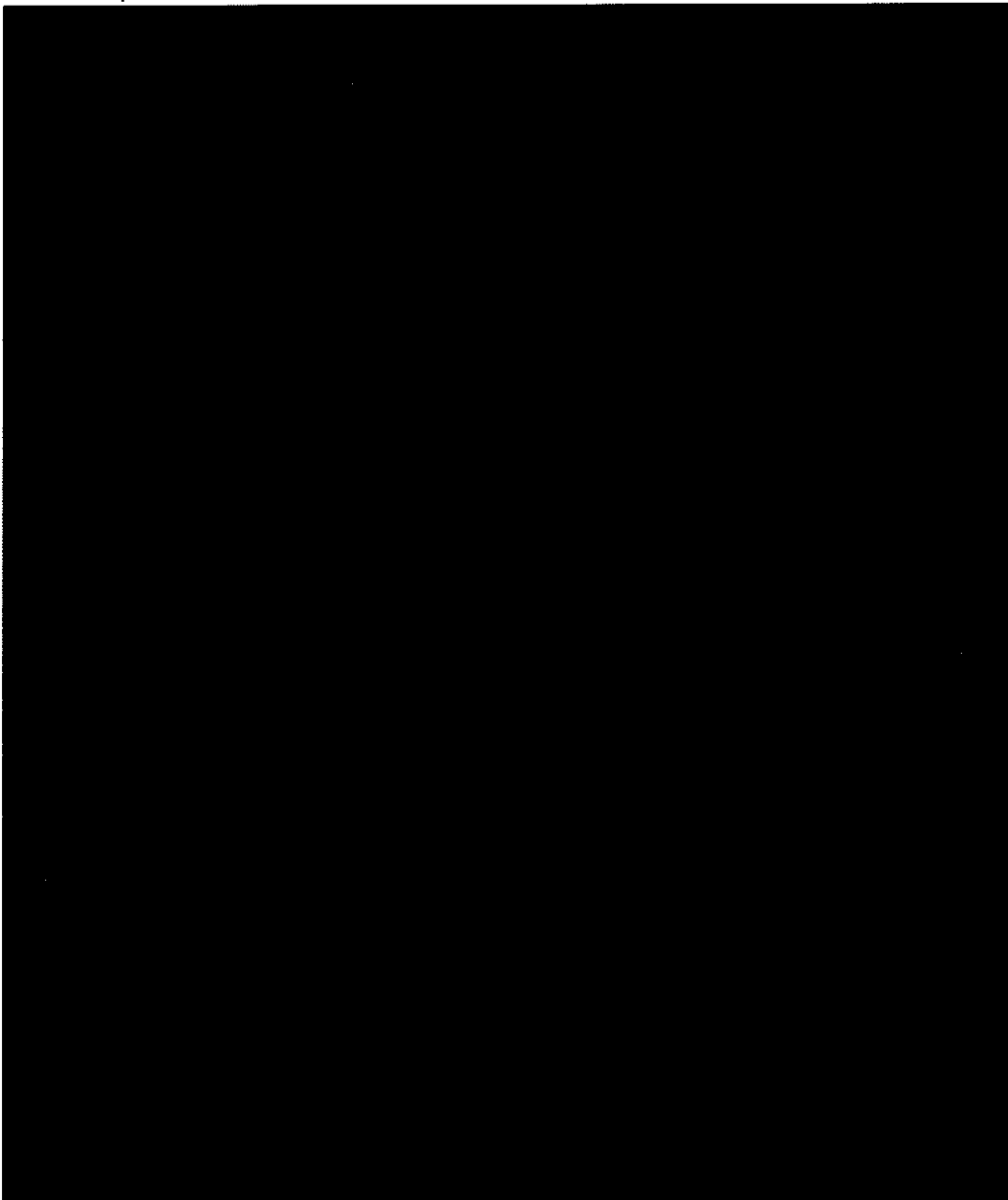
(b) the targets of this electronic surveillance, **Various Known and Unknown Agents of**

 presumed U.S. persons, described

in Exhibit A to the application, are agents of this foreign power, as defined by 50 U.S.C.

§ 1801(b)(2)(E) [50 U.S.C. § 1805(a)(3)(A)];

(c) each of the following telephone numbers,



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

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



at which the electronic surveillance is directed, is being used or is about to be used by

Various Known and Unknown Agents of [REDACTED]

[REDACTED] **presumed U.S. persons**, and electronic surveillance is authorized, using

for each facility either or both of the means identified below [50 U.S.C. § 1805(a)(3)(B)];

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

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

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

5. The application 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)].

The Court understands that the Government expects to file emergency FISA applications pursuant to 50 U.S.C. § 1805(f) seeking authority to intercept international communications to and from additional telephone numbers reasonably believed to be used by persons in the United States, where there arises probable cause to believe that such numbers are being used or are about to be used by known and unknown agents of [REDACTED]

[REDACTED] The Court understands that the Government has proposed a streamlined FISA emergency application form, attached as Exhibit G to the application, specifically and exclusively for this purpose. The Court finds that for any such application made under docket number [REDACTED] b(7)(E) the form of this proposed application is consistent with FISA subject to § 1805(d).

The Court also understands that the effectiveness of the surveillance proposed in this application and subsequent emergency applications made under this docket depends upon the manner of its operation remaining unknown to terrorists, and that it is critical to United States' counterterrorism operations that agents of [REDACTED] subject to such surveillance do not learn that they have been identified by the Government. The Court accordingly determines that the Government has established "good cause" within the meaning of section 1806(j) of Title 50 that a subject of emergency surveillance initiated by the Government

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

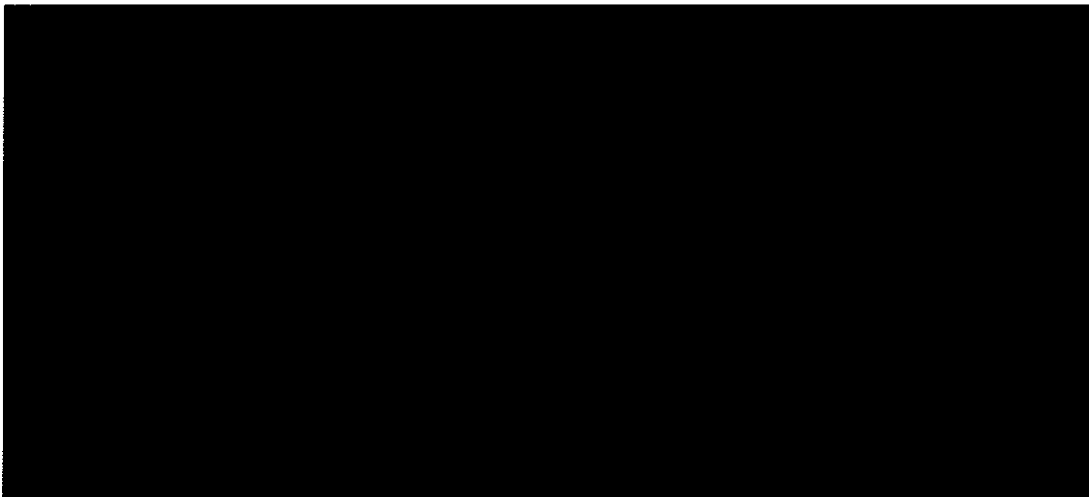
~~TOP SECRET//COMINT//NOFORN~~

during the period of this Order, but not authorized by this Court, should not be notified of the emergency employment of electronic surveillance. For any such surveillance, the requirement of notice shall be suspended for ninety days following the emergency employment of electronic surveillance, provided that on a further ex parte showing of good cause by the Government, the Court shall forgo ordering the serving of the notice required under section 1806 (j) of Title 50.

WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States to conduct electronic surveillance, as described in the application, is GRANTED, and it is

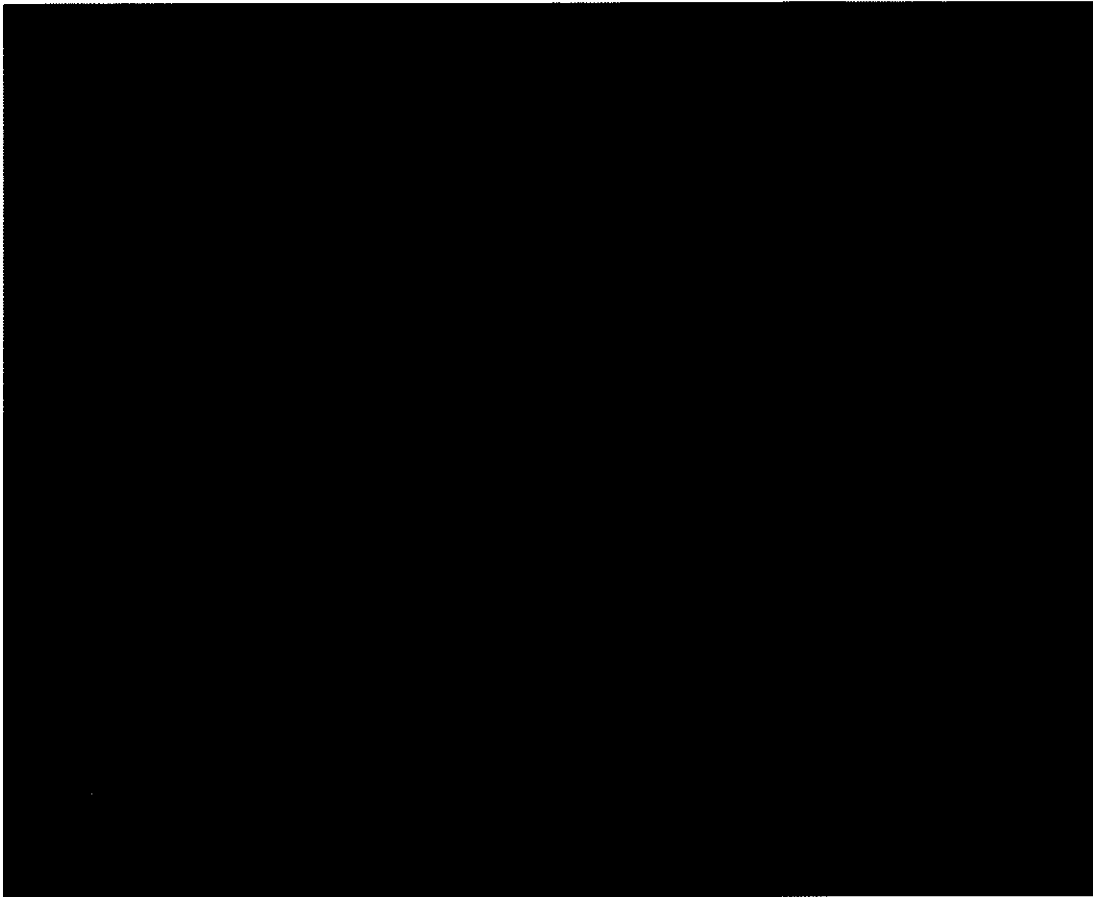
FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

(1) The United States is authorized 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 and specifically detailed in paragraph (3) below, for a period of **ninety days**, unless otherwise ordered by the Court, as follows:

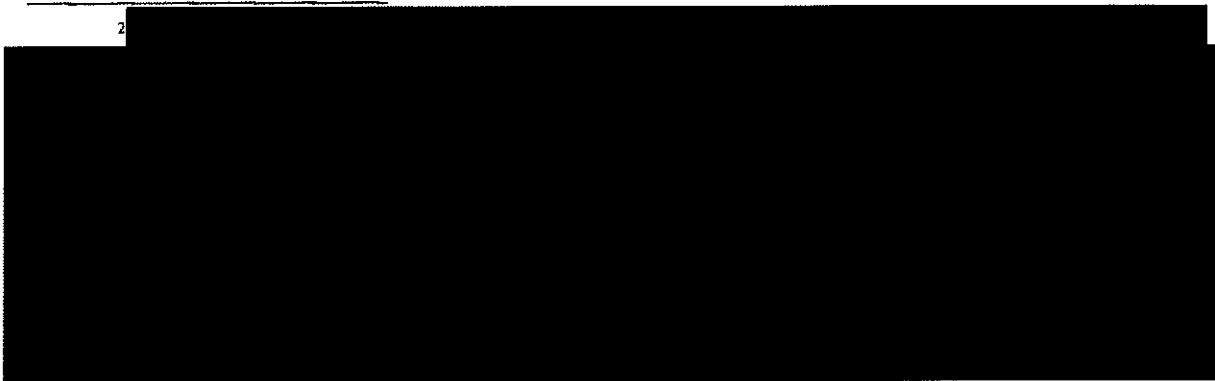


~~TOP SECRET//COMINT//NOFORN~~

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



2



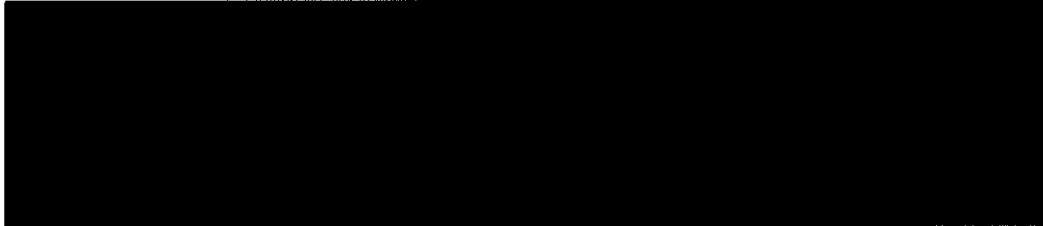
³ Although the NSA surveillance will be designed to acquire only international communications where one communicant is outside the United States, the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that no domestic communications will be acquired. 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~~

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:



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, or granted under any subsequent authorization made in connection with this docket number, all in accordance with the order 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:

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

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

(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.

(b) [REDACTED]
[REDACTED]
[REDACTED]
[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

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

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

(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.

(b) Certain of the modifications to the standard NSA FISA minimization procedures adopted by this Court in *In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets*, Order, No. (7)(E) (May 10, 2002) ("*Raw Take Motion*"), which modifications are set forth below:

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

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

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

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:⁴

(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.

⁴ and b(7)(E)

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

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

5. The following shall be added to the 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 these standard NSA FISA procedures:

1. Notwithstanding sections 3(c)(2) and (e), 5(b), and 6(a) of these standard NSA FISA procedures, communications acquired under this Order may be retained for five years, unless this Court approves retention for a longer period.

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~~

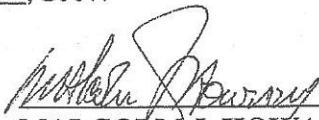
~~TOP SECRET//COMINT//NOFORN~~

(4) The CIA shall minimize all communications received under this Order as provided in Exhibit F to the application.

Signed 10 JAN 2007, 4:15 pm Eastern Time
Date Time

This authorization regarding Various Known and Unknown Agents of [REDACTED]

[REDACTED] presumed U.S. persons, expires at 3:00 pm
on the 6th day of APRIL, 2007.


MALCOLM J. HOWARD
Judge, United States Foreign
Intelligence Surveillance Court

b(6) and b(7)(C) Deputy Clerk
FISC. certify that this document
is a true and correct copy of
the original b(6) and
b(7)(C)

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

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE [REDACTED] :

[REDACTED] : Docket No.: (b)(7)(E)

:

:

ORDER AND MEMORANDUM OPINION

This case involves an extremely important issue regarding probable cause findings that determine what persons and what communications may be subjected to electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), 50 U.S.C. §§ 1801-1811: Are they required to be made by a judge of this Court, through procedures specified by statute for the issuance of a FISA order under 50 U.S.C. § 1805? Or may the National Security Agency (NSA) make these probable cause findings itself, as requested in the application in this case, under an alternative mechanism adopted as "minimization procedures"?¹

I. INTRODUCTION

When the government believes that a telephone number or e-mail address is being used in furtherance of international terrorism, it will appropriately want to acquire communications relating to that number or e-mail address. Under FISA, the government may obtain an electronic surveillance order from this Court, upon a judge's finding, *inter alia*, of probable cause to believe that the telephone number or e-mail address is used by a foreign power (to include an international terrorist group) or an agent of a foreign power. § 1805(a)(3)(B). In an emergency, the government may begin the electronic surveillance before obtaining the Court order, upon the approval of the Attorney General and provided that a Court order, supported by such a judicial probable cause finding, is obtained within 72 hours thereafter. § 1805(f).

Until recently, these were the only circumstances in which the government had sought, or this Court had entered, a FISA order authorizing electronic surveillance of the telephone or e-

¹ This order and opinion rests on an assumption, rather than a holding, that the surveillance at issue is "electronic surveillance" as defined at 50 U.S.C. § 1801(f), and that the application is within the jurisdiction of this Court. See note 12 *infra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

mail communications of suspected international terrorists. However, on December 13, 2006, in Docket No. [REDACTED], the government filed an application seeking an order that would authorize electronic surveillance of telephone numbers and e-mail addresses thought to be used by international terrorists without a judge's making the probable cause findings described above, either before initiation of surveillance or within the 72 hours specified in § 1805(f). The proposed electronic surveillance targeted [REDACTED] and involved acquisition by NSA of international telephone and Internet communications [REDACTED].

That application was presented to another judge of this Court. After considering the application and supporting materials, that judge orally advised the government that he would not authorize, on the terms proposed in the application, electronic surveillance of "selector" phone numbers and e-mail addresses, as described below, believed to be used by persons in the United States. The government then filed a second application regarding surveillance of the previously identified phone numbers used by persons in the United States on January 9, 2007, in Docket No. [REDACTED].

On January 10, 2007, the judge entered orders in Docket No. [REDACTED] that granted the requested electronic surveillance authority, subject to a number of modifications, and specifically limiting the authorized surveillance to "selector" phone numbers and e-mail addresses believed to be used by persons outside the United States. Primary Order at 12. On the same date, the judge also entered orders granting the surveillance authority requested by the application in Docket No. [REDACTED] for the identified phone numbers believed to be used by persons in the United States.

The authorization in Docket No. [REDACTED] comported with the long-established probable cause determination described above, but the authorization in Docket No. [REDACTED] did not. The Primary Order in Docket No. [REDACTED] identified [REDACTED] phone numbers as the facilities at which the electronic surveillance is directed and, pursuant to § 1805(a)(3)(B), found probable cause to believe that each phone number was being used or about to be used by an agent of a foreign power. Primary Order at 4-5. This finding rested on specific facts provided in the application regarding the use of each phone number.²

² Declaration of [REDACTED] NSA, at 4-59 (Exhibit A to application in Docket No. [REDACTED]). In subsequent supplemental orders, the judge authorized additional phone numbers for surveillance in Docket No. [REDACTED] based on the same kind of judicial probable cause findings, for a total of [REDACTED] telephone numbers covered in Docket No. [REDACTED]. See, e.g., Amendment to Order at [REDACTED] (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

On the other hand, the Primary Order in Docket No. [REDACTED] did not identify, or make probable cause findings regarding, [REDACTED] phone numbers and e-mail addresses subject to surveillance under that order. Instead, that order identified [REDACTED] which the authorized electronic surveillance is directed and found probable cause to believe that [REDACTED] was being or about to be used by the targeted terrorist organizations. Docket No. [REDACTED] Primary Order at 2-5.

On March 21, 2007, the government filed the application in this case, Docket No. [REDACTED] seeking renewal of the surveillance authority granted in Docket No. [REDACTED].³ This application follows Docket No. [REDACTED] in identifying [REDACTED] which the electronic surveillance is directed for purposes of the judge's probable cause findings under § 1805(a)(3)(B).⁴

II. THE SURVEILLANCE AT ISSUE

For surveillance of international telephone communications, [REDACTED] identified in the application. Alexander Decl. at 16. The devices acquire only communications to or from the telephone numbers entered as "selectors." Alexander Decl. at 16, 20-21.

²(...continued).

2 (entered Jan. 16, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Jan. 22, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Feb. 2, 2007).

³ On March 22, 2007, in Docket No. [REDACTED], the government filed an application for renewal of the authority granted in Docket No. [REDACTED]. The renewal application identifies [REDACTED] U.S. phone numbers as the facilities at which the surveillance is directed, and requests that the Court find probable cause to believe that each of these phone numbers is being used or is about to be used by an agent of a foreign power, based on specific information set out in the application regarding the use of each number. Docket [REDACTED], proposed Order at 2-5, Declaration of [REDACTED] NSA, at 6-64 (submitted as Exhibit A to Application).

⁴ Docket No. [REDACTED], Application at 4-5; Declaration of Lt. Gen. Keith B. Alexander, Director, NSA, at 26-42 (submitted as Exhibit C to Application) (hereinafter "Alexander Decl."); proposed Order at 6.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

For Internet communications, NSA uses e-mail addresses as selectors.⁵ [REDACTED]

[REDACTED] Id. at 34-42. [REDACTED] acquire only communications that are to or from, or that contain a reference to,⁶ a selector e-mail address. Id. at 14-15, 21-23.

NSA uses telephone numbers or e-mail addresses as selectors only if "it reasonably believes [they] are being used or are about to be used by persons located overseas and . . . has determined there is probable cause to believe [they] are being used or about to be used by a member or agent of [REDACTED]"

[REDACTED] Id. at 43. The government submits that applying this standard for selectors "narrowly focus[es] NSA's collection efforts on communications" of the targeted terrorist groups, id. at 15. [REDACTED]

[REDACTED] Id. at 14. [REDACTED] overseas e-mail addresses and phone numbers have been adopted as selectors under this standard pursuant to the order in Docket No. [REDACTED] (b)(7)(E). Id. at 19.

In most relevant respects, the means of electronic surveillance at issue in this case are quite similar to how [REDACTED] FISA surveillance orders have been implemented. The means of conducting the phone surveillance is, for all relevant purposes, indistinguishable from many prior cases in which communications to or from particular phone numbers are acquired by use of [REDACTED]

[REDACTED] The e-mail surveillance is also quite similar to what has been [REDACTED]

⁵ [REDACTED]

⁶ This surveillance acquires an Internet communication containing a reference to a selector e-mail address [REDACTED]

[REDACTED] Id. at 22 n.34.

⁷ [REDACTED]

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorized previously, to the extent that it acquires communications to or from selector e-mail addresses.⁸ The acquisition of e-mail communications because they refer to a selector e-mail

⁷(...continued)

[REDACTED]

In addition, the standard description of ^{b(1), b(7)(E)} ^{b(1), b(7)(E)} conducted by the FBI states that such surveillance and b(6) and b(7)(C)

[REDACTED]

⁸

[REDACTED]

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

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

address does not appear to have been authorized under FISA prior to Docket No. [REDACTED] and is discussed further below.

III. PROBABLE CAUSE FINDINGS

Under FISA, a judge of this Court may enter an electronic surveillance order only upon finding, inter alia, that

on the basis of the facts submitted by the applicant there is probable cause to believe that --

(A) the target⁹ of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) 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.

§ 1805(a)(3) (emphasis added). FISA defines "foreign power," in relevant part, as including "a group engaged in international terrorism or activities in preparation therefor." § 1801(a)(4).

In this case, the government contends that, for purposes of § 1805(a)(3)(B) the "facilities" at which the electronic surveillance is directed are [REDACTED] E.g., Alexander Decl. at 13; Government's Memorandum of Law at 32 (attached to Application as part of Exhibit A). The government acknowledges that the telephone numbers and e-mail addresses selected for

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

[REDACTED]

⁹ The target of a surveillance "'is the individual or entity . . . about whom or from whom information is sought.'" In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, pt. 1 at 73 (1978)).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

acquisition are [REDACTED] "facilities" [Government's Memorandum of Law at 31 n.18] [REDACTED] Simultaneously, however, the government maintains in another case that [REDACTED] resulting in an entirely different focus for the judge's assessment of probable cause under § 1805(a)(3)(B).¹⁰ Underlying the government's position, therefore, is the premise that § 1805(a)(3)(B) can be applied so variously that a FISA judge has great discretion in determining what "facilities" should be the subject of the judge's probable cause analysis.

In deciding how to apply § 1805(a)(3)(B), the Court looks first to the language of the statute. See, e.g., Engine Manufacturers Ass'n v. South Coast Air Quality Mgmt. Dist., 541 U.S. 246, 252 (2004). That statutory language specifies that a probable cause finding must be made for each facility "at which the electronic surveillance is directed." The statute provides four alternative definitions of electronic surveillance, but the one most pertinent to this case is at § 1801(f)(2).¹¹ Section 1801(f)(2) defines "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition

¹⁰ For example, the manner of phone surveillance [REDACTED] proposed in this docket is identical to that proposed in Docket No. [REDACTED] for phone numbers used in the United States. Compare Docket No. [REDACTED] Declaration of Lt. Gen. Keith B. Alexander, Director, NSA at 3 (submitted as Attachment C to Application) (defining [REDACTED] with Alexander Decl. in this docket at 24-25 (same definition, but with references to [REDACTED] and to the "minimization probable cause standard"). [REDACTED] and b(7)(E)

[REDACTED] Proposed Order at 2-6.

¹¹ Section 1801(f)(2) provides the relevant definition of "electronic surveillance" for all of the proposed phone surveillance, as well as the proposed e-mail surveillance [REDACTED] Application at 19. In the government's view, the relevant definition for [REDACTED] See note 13 *infra* & accompanying text.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

occurs in the United States.” (Emphasis added.)¹² Thus, the electronic surveillance is the acquisition of the contents of communications.

In this case, communications will be acquired because they are to or from (or, in the case of Internet communications, refer to) a certain class of facilities - - - the telephone numbers and e-mail addresses used as selectors. NSA has no interest in acquiring the contents of [REDACTED]

Rather, it is interested in acquiring only [REDACTED] Accordingly, NSA [REDACTED] to select for acquisition communications that relate to a selector facility, and to exclude from acquisition [REDACTED]

¹² The record does not disclose to what extent the surveillance conducted under Docket No. [REDACTED] b(7)(E) has in fact acquired communications to or from a person in the United States. See Alexander Decl. at 22 n.36 (the “volume of communications targeted for collection” in Docket No. [REDACTED] b(7)(E) makes it “technically infeasible” to provide such information, but “a central purpose” of such surveillance “is to collect communications to or from terrorist operatives in the United States”). However, given the large number of selectors involved [REDACTED]

[REDACTED] it appears likely that this surveillance would acquire some indeterminate number of communications to or from persons in the United States. See, e.g., id. at 6-8 [REDACTED]

In view of this apparent likelihood, the government’s implicit request that the Court exercise jurisdiction over the submitted application, the Court’s prior acceptance of jurisdiction in Docket No. [REDACTED] b(7)(E) and prior decisions of this Court that have accepted jurisdiction in similar cases [REDACTED] and [REDACTED] b(7)(E)

[REDACTED] I assume for purposes of this order and opinion that this case does involve “electronic surveillance” as defined by FISA, such that this Court has jurisdiction. However, I believe that the jurisdictional issues regarding the application of FISA to phone numbers and e-mail addresses that are used exclusively outside the United States merit further examination. I further believe that Congress should also consider clarifying or modifying the scope of FISA and of this Court’s jurisdiction with regard to such facilities, given the large number of overseas e-mail addresses and phone numbers now identified by the government for surveillance, and the government’s assertions regarding the need for speed and agility in targeting such facilities as new ones are identified in the future. See pages 18-19 infra.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] These facts strongly suggest that the acquisition of the contents of communications - - - that is, the electronic surveillance itself - - - is directed at the telephone numbers and e-mail addresses used as selectors.

In the government's view, a discrete part of the proposed e-mail surveillance, to be conducted [REDACTED] should be analyzed under the definition of "electronic surveillance" provided at § 1801(f)(4).¹³ Section 1801(f)(4) defines "electronic surveillance" to include "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication . . ." (Emphasis added.) A similar analysis applies under § 1801(f)(4): because the surveillance consists of monitoring to acquire information, and the only information to be acquired relates to the e-mail addresses used as selectors, the electronic surveillance would be directed at those e-mail addresses.

The government argues to the contrary that this surveillance is not [REDACTED]

[REDACTED] Government's Memorandum of Law at 32. But, nothing in the language of the statute identifies the facility at which the surveillance is directed [REDACTED] Congress could have used language that focused [REDACTED] but chose not to do so in § 1805(a)(3)(B). Compare § 1842(d)(2)(A)(iii) (requiring FISA pen register/trap and trace orders to specify, "if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied") (emphasis

¹³ The orders in Docket No. [REDACTED] authorized surveillance [REDACTED] but NSA has not commenced such surveillance. NSA intends to do so within the next 90 days, but has not determined how such surveillance will be conducted, or even whether some part of its intended activity will involve [REDACTED] Alexander Decl. at 41 nn.49 & 52, 42 n.55.

¹⁴ Certainly the term "directed" cannot be construed to do so. See Webster's II New College Dictionary 321 (2001) (defining "direct" to mean, inter alia, "To move or guide (someone) toward a goal;" "To show or indicate the way to;" "To cause to move in or follow a direct or straight course <directed the arrow at the bull's-eye>," "To address (e.g., a letter) to a destination.")

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

added). And, the relevant provisions assign no significance to the place where communications are acquired, so long as acquisition "occurs in the United States" (as is the case here).¹⁵

The government further argues that one portion of the proposed surveillance - - - the acquisition of e-mails that contain a reference to, but are not to or from, a selector e-mail address - - - cannot be conducted [REDACTED]

[REDACTED] Government's Supplemental Memorandum of Law at 6-7 (submitted as part of Exhibit A to the Application).¹⁶ However, even for this part of the surveillance, communications [REDACTED]

[REDACTED] The surveillance functions in this way because NSA is not interested in the contents of communications [REDACTED]; rather, it is only interested in the contents of those communications (to include the e-mail addresses of the communicants) that refer to a selector e-mail address. For these reasons, I find that this aspect of the proposed surveillance is not [REDACTED], but rather at particular e-mail addresses.¹⁷

The government also cites several prior cases as precedent for the interpretation of § 1805(a)(3)(B) adopted in Docket No. [REDACTED] b(7)(E). These cases involved very different

¹⁵ § 1801(f)(2); see also § 1801(f)(4) ("installation or use of a[] . . . surveillance device in the United States . . .")

¹⁶ The government identifies [REDACTED] communications acquired by this aspect of the surveillance. Government's Supplemental Memorandum of Law at 6-7; Declaration of [REDACTED] b(3), b(6) and b(7) NSA ("b(3) Decl.") at 16-18 (submitted as part of Exhibit A to the Application). [REDACTED] and b(6) and b(7) [REDACTED]

¹⁷ On the record before me, I cannot, and do not, decide exactly which particular e-mail addresses are the ones at which this type of surveillance is directed. To the extent it is concluded that surveillance is directed at e-mail addresses [REDACTED] a judge would have to find probable cause to believe that those e-mail addresses, [REDACTED] are being used or are about to be used by a foreign power or an agent of a foreign power before authorizing the surveillance proposed in the application.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

circumstances, such as surveillances that acquired

Tellingly, none

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

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

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

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

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of the cited cases stand for the proposition on which this application rests - - - that electronic surveillance is not "directed" at particular phone numbers and e-mail addresses. [REDACTED]

Moreover, in each of the cited cases involving surveillance under § 1805,²⁰ the judge made probable cause determinations that a single target or well-defined set of targets [REDACTED]

[REDACTED] These determinations constrained the ability of executive branch officials to direct surveillance against persons and communications of their unilateral choosing in a way that, as discussed below, the proposed probable cause findings in this case would not.

Therefore, I conclude that, under the plain meaning of §§ 1805(a)(3)(B) and 1801(f), the proposed electronic surveillance is directed at the telephone numbers and e-mail addresses used as selectors. The result of applying this plain meaning is by no means absurd.²¹ and b(7)(E) [REDACTED]

¹⁹(...continued)

and b(7)(E) [REDACTED]

²⁰ One case relied on by the government involved different statutory requirements and no probable cause finding at all. [REDACTED]

[REDACTED] Docket No. PR/TT ^{b(7)(E)} involved the use of pen registers and trap and trace devices to acquire addressing and routing information, not the full content of communications. Because issuing a FISA pen register/trap and trace order under § 1842 does not require the judge to make probable cause findings, the Opinion and Order entered on July 14, 2004, at 49 n.34, expressly disclaimed any application to full-content surveillances under § 1805.

²¹ See Laimie v. United States Trustee, 540 U.S. 526, 534 (2004) (court is to enforce plain language of a statute, "at least where the disposition required by the text is not absurd") (internal quotations omitted).

²² See notes 7 and 8 supra.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and b(7)(E) [REDACTED] cases (other than
this case and Docket No. [REDACTED]) consistently reflect the same understanding [REDACTED]
[REDACTED]

However, even if the statutory language were as elastic as the government contends, it would still be incumbent on me to apply the language in the manner that furthers the intent of Congress. In determining what interpretation would best further congressional intent, it is appropriate to consult FISA's legislative history.²⁵ That legislative history makes clear that the

²³ See, e.g., In re [REDACTED] and b(6), b(7)(C), and (E)

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

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

²⁵ See Train v. Colorado Public Interest Research Group, 426 U.S. 1, 10 (1976).
Moreover, if § 1805(a)(3)(B) could be applied in such widely varying ways to the same surveillance, then its terms would be sufficiently unclear that legislative history may be consulted
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

purpose of pre-surveillance judicial review is to protect the fourth amendment rights of U.S. persons.²⁶ Congress intended the pre-surveillance "judicial warrant procedure," and particularly the judge's probable cause findings, to provide an "external check" on executive branch decisions to conduct surveillance.²⁷

Contrary to this intent of Congress, the probable cause inquiry proposed by the government could not possibly restrain executive branch decisions to direct surveillance at any particular individual, telephone number or e-mail address. Under § 1805(a)(3)(B), the government would have the Court assess [REDACTED]

[REDACTED] See Alexander Decl. at 6-8, 11-12], and make a highly abstract and generalized probable cause finding [REDACTED] However, such a probable cause finding could be made with equal validity [REDACTED]

²⁵(...continued)

to ascertain their proper meaning. See, e.g., Blum v. Stenson, 465 U.S. 886, 896 (1984).

²⁶ "A basic premise behind this bill is the presumption that whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate." E.g., H. Rep. 95-1283, pt. 1, at 24-25; see also id. at 26 (purpose of extending warrant procedure to surveillances targeting non-U.S. persons "would not be primarily to protect such persons but rather to protect U.S. persons who may be involved with them"). Such protection was deemed necessary in view of prior abuses of national security wiretaps. Id. at 21 ("In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties.").

²⁷

The bill provides external and internal checks on the executive. The external check is found in the judicial warrant procedure which requires the executive branch to secure a warrant before engaging in electronic surveillance for purposes of obtaining foreign intelligence information. . . . For such surveillance to be undertaken, a judicial warrant must be secured on the basis of a showing of "probable cause" that the target is a "foreign power" or an "agent of a foreign power." Thus the courts for the first time will ultimately rule on whether such foreign intelligence surveillance should occur.

S. Rep. 95-604, pt. 1, at 16, reprinted in 1978 U.S.C.C.A.N. 3904, 3917.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] On this reading of § 1805(a)(3)(B), facts supporting or contradicting the government's belief that terrorists use the phone numbers and e-mail addresses for which information will be acquired are irrelevant to the judge's probable cause findings.²⁸

Thus, under the government's interpretation, the judge's probable cause findings have no bearing on the salient question: whether the communications to be acquired will relate to the targeted foreign powers.²⁹ As discussed below, the government would have all of the probable cause findings bearing on that question made by executive branch officials, subject to after-the-fact reporting to the Court, through processes characterized by the government as minimization. That result cannot be squared with the statutory purpose of providing a pre-surveillance "external check" on surveillance decisions, or with the expectation of Congress that the role of the FISA judge would be "the same as that of judges under existing law enforcement warrant procedures."³⁰

²⁸ The government argues that the Court has previously, and should here, apply the requirements of § 1805(a)(3) in a flexible, common-sense fashion. See, e.g., Government's Supplemental Memorandum of Law at 12-14. In some cases, the Court's probable cause findings have left the government with a degree of flexibility in precisely how the surveillance is directed

[REDACTED] But, none of the cited cases approach what the government proposes here - - - findings under § 1805(a)(3) that do nothing to limit the government's discretion regarding the persons effectively targeted for surveillance or the communications to be acquired by the surveillance.

²⁹ Judicial authorization and oversight of surveillance under FISA is analogous to the judicial role in domestic criminal surveillance under Title III. After comparing § 1805(a)(3)(B) with the requirements for a Title III wiretap, the Foreign Intelligence Surveillance Court of Review concluded: "FISA requires less of a nexus between the facilities and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." In re Sealed Case, 310 F.3d at 740 (emphasis added). However, under the government's theory, the judge's probable cause findings have no bearing whatever on whether the communications actually acquired pertain to a target.

³⁰ H. Rep. 95-1283, pt. 1, at 25. Congress expected the judge to "assess the facts to determine whether certain of the substantive standards have been met," in "the traditional role of a judge in passing on a warrant application." Id.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

The government's proposed probable cause findings under § 1805(a)(3)(A) do not alter these conclusions. No matter how well-founded, a judge's assessment of probable cause to believe that [REDACTED] are foreign powers cannot, in the context of the government's proposal, provide any check on what or whose communications are intercepted.³¹ These foreign powers can only communicate (or otherwise act) through individual members or agents, who use particular phone numbers and e-mail addresses. Because none of the probable cause findings proposed by the government, under either prong of § 1805(a)(3), concerns these particular individuals, phone numbers, or e-mail addresses, the judge's role in making such findings cannot provide the "external check" intended by Congress.

Accordingly, I must conclude that, for purposes of § 1805(a)(3)(B), the phone numbers and e-mail addresses used as selectors are facilities at which the electronic surveillance is directed. I am unable, "on the basis of the facts submitted by the applicant," to find probable cause to believe that each of these facilities "is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* The application contains no facts that would support such a finding. Instead, it is represented that NSA will make the required probable cause finding for each such facility before commencing surveillance. Alexander Decl. at 43. The application seeks, in effect, to delegate to NSA the Court's responsibility to make such findings "based on the totality of circumstances." *See* proposed Order at 14-15.³² Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order.³³

³¹ *See* S. Rep. 95-701 at 54, reprinted in 1978 U.S.C.C.A.N. 3973, 4023 (requirement that "the court, not the executive branch, make[] the finding of whether probable cause exists that the target of surveillance is a foreign power or its agent" is intended to be a "check[] against the possibility of arbitrary executive action").

³² *Compare, e.g.,* H. Rep. 95-1823, pt. 1, at 43 ("judge is expected to take all the known circumstances into account" in assessing probable cause to believe that an individual is an agent of an international terrorist group) (emphasis added).

³³ This analysis of congressional purpose applies equally to the aspect of the surveillance that acquires communications that refer to a selector e-mail address, and supports the conclusion that such surveillance is not [REDACTED] identified by the government. This order and opinion does not decide which e-mail addresses are facilities at which such surveillance is directed. *See* note 17 *supra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

IV. MINIMIZATION

Another requirement for an electronic surveillance order under § 1805 is that the Court must also find that "the proposed minimization procedures meet the definition of minimization procedures under section 1801(h)." § 1805(a)(4). That section defines minimization procedures, in pertinent part, as

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.

§ 1801(h)(1). FISA minimization procedures cannot be framed "in a way that is clearly inconsistent with the statutory purpose." In re Sealed Case, 310 F.3d at 730. More importantly, the minimization procedures must be consistent with the statutory text. See, e.g., Laimie, 540 U.S. at 538 (stressing the "difference between filling a gap left by Congress' silence and rewriting rules that Congress has affirmatively and specifically enacted") (internal quotations omitted). Accordingly, proposed minimization procedures that conflict with other provisions of FISA cannot be "reasonably designed" within the meaning of § 1801(h)(1).³⁴

It follows from this principle, and from the foregoing analysis of § 1805(a)(3)(B), that the record in this case will not support the finding required by § 1805(a)(4). The minimization procedures first approved in Docket No. [REDACTED] and proposed in this matter conflict with specific provisions of FISA that govern the initiation and extension of electronic surveillance authority. For example, under the proposed procedures, NSA may initiate surveillance of a foreign phone number or e-mail address unilaterally; express judicial approval is not required,

³⁴ This conclusion holds even if the proposed procedures arguably concern the "acquisition" of information under § 1801(h)(1). All of 50 U.S.C. §§ 1801-1811 regulates the acquisition of information by electronic surveillance. The requirement to adopt and follow reasonable minimization procedures is in addition to the statute's other requirements for authorizing electronic surveillance, including the requirement that the judge make the probable cause findings specified at § 1805(a)(3). Minimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

even after the fact.³⁵ However, § 1805(f) provides that emergency approvals can only be granted by the Attorney General,³⁶ after which an application for electronic surveillance authority must be presented to a judge of this Court within 72 hours of emergency authorization, and surveillance must terminate within 72 hours of the emergency authorization unless a Court order, supported by the necessary probable cause findings, is obtained.

The proposed minimization procedures are also inconsistent with other express statutory requirements regarding the duration and extension of surveillance authorizations. Surveillances targeting foreign powers as defined by § 1801(a)(4) may be initially authorized for up to 90 days [§ 1805(e)(1)] and “extensions may be granted . . . upon an application for an extension and new findings made in the same manner as required for an original order.” § 1805(e)(2). Such “findings” must include a judge’s finding of probable cause to believe that each phone number or e-mail address at which surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power. However, the proposed procedures make no provision for review of probable cause at any time after the surveillance is first reported to the Court.

The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute.

The government argues that alternative, extra-statutory procedures are necessary to provide or enhance the speed and flexibility with which NSA responds to terrorist threats. Government’s Memorandum of Law at 11-12; Government’s Supplemental Memorandum of Law at 4-5. It notes that, in the time it takes to get even an Attorney General emergency

³⁵ A report “briefly summariz[ing] the basis” for NSA’s probable cause findings in support of surveillance of new phone numbers and e-mail addresses would be submitted to the Court at 30-day intervals. Application at 8-9. If the Court concluded that there is not probable cause to believe that such a phone number or e-mail address is used by a targeted foreign power, it could direct that surveillance terminate “expeditiously.” *Id.* at 9.

³⁶ “Attorney General” is defined at § 1801(g) to include also the Acting Attorney General, the Deputy Attorney General, and, “upon designation,” the Assistant Attorney General for National Security.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorization, vital foreign intelligence information may be lost. Government's Memorandum of Law at 11-12; Alexander Decl. at 20; [REDACTED] Decl. at 13-15. These matters concern me as well. But, these are risks that Congress weighed when it adopted FISA's procedural requirements,³⁷ over dissenting voices who raised some of the same concerns the government does now.³⁸ These requirements reflect a balance struck by Congress between procedural safeguarding of privacy interests and the need to obtain foreign intelligence information.

The procedures approved in Docket No. [REDACTED] b(7)(E) and proposed in this application strike this balance differently for surveillance of phone numbers and e-mail addresses used overseas. However, provided that a surveillance is within the scope of FISA at all,³⁹ the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States. Congress could well take note of the grave threats now presented by international terrorists and changes in the global communications system,⁴⁰ and conclude that FISA's current requirements are unduly burdensome for surveillances of phone numbers and e-mail addresses used overseas.⁴¹ Unless and until legislative action is taken, however, the judges of this Court must apply the procedures set out in the statute. See § 1803(a) (Court has "jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter") (emphasis added).

³⁷ See H.R. Rep. 95-1283, pt. 1, at 26 (acknowledging potential "risks of impeding or barring needed intelligence collection").

³⁸ FISA's "warrant requirement . . . would pose serious threats to the two most important elements in effective intelligence gathering: (1) speed and (2) security The real possibilities of delay . . . are risks the intelligence community should not be required to take." *Id.* at 113 (Dissenting views of Reps. Wilson, McClory, Robinson, and Ashbrook).

³⁹ This condition is assumed, but not decided, for purposes of this order and opinion. As noted elsewhere, I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States. See note 12 *supra*.

⁴⁰ See, e.g., Alexander Decl. at 11 ([REDACTED])

⁴¹ *Id.* at 19 (burden of preparing FISA applications for [REDACTED]); Government's Supplemental Memorandum of Law at 4 (same); [REDACTED] b(3) Decl. at 13-14 (same).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Fidelity to this principle "allows both [the legislative and judicial] branches to adhere to our respected, and respective, constitutional roles." Laimie, 540 U.S. at 542.

For the foregoing reasons, I conclude that I cannot grant the application in Docket No. [REDACTED] in the form submitted. I recognize that the government maintains that the President may have "constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization." Application at 25 n.12; see also Alexander Decl. at 6 n.6

[REDACTED] Nothing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters.

V. REQUEST FOR LEAVE TO SEEK EXTENSION IN DOCKET NO. [REDACTED]

On March 29, 2007, I orally advised attorneys for the government that, after careful review of the application and supporting materials, I had reached the above-stated conclusion, and provided a brief summary of the reasoning more fully stated herein. I also stated that, if it chose to do so, the government could supplement the record at a formal hearing.

Based on ensuing discussions, I believe that the government may be able to submit a revised and supplemented application, on the basis of which I could grant at least a substantial portion of the surveillance authorities requested herein, consistent with this order and opinion. The government has undertaken to work toward that goal; however, it is understood that the government has not yet decided on a particular course of action and may, after further consideration, conclude that it is not viable to continue this surveillance within the legal framework stated in this order and opinion.

On April 2, 2007, the government filed in the above-captioned docket a Motion for Leave to File an Application for an Extension of the Orders Issued in Docket No. [REDACTED]. That motion requests leave to file an application for a 60-day extension of those authorities. Motion at 3. On April 3, 2007, the government informally advised that it did not wish to have a hearing on the record prior to my ruling on the motion. I have decided to grant the government leave to file such an application in Docket No. [REDACTED], subject to the requirements stated below.

The sole purpose for granting such leave is to give the government a reasonable amount of time to work in good faith toward the preparation and submission of a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in Docket No. (b)(7)(E), on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of (b)(7)(E) phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion.

Accordingly, it is hereby ORDERED as follows:

(1) The government may submit an application for a single extension of the authorities granted in Docket No. (b)(7)(E). Any authorities granted pursuant to such an application shall terminate no later than 5:00 p.m., Eastern Time, on May 31, 2007. There shall be no extensions beyond May 31, 2007.

(2) If an extension is obtained under paragraph (1), the government shall periodically submit written reports to me regarding its efforts to prepare and submit for my consideration a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. The first report shall be submitted on or before April 20, 2007; the second report shall be submitted on or before May 4, 2007; and the third report shall be submitted on or before May 18, 2007.

(3) If, during the period of an extension obtained under paragraph (1), the government determines that it is not feasible or not desirable to submit a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, it shall immediately notify me in writing of this determination. The submission of such notification shall relieve the government of the requirement to submit reports under paragraph (2). I contemplate that, upon receipt of such notification, I would enter an order formally denying the application in the above-captioned docket.

(4) If authorities obtained pursuant to any extension under paragraph (1) should expire before the government has submitted, and I have ruled on, a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, then this order and opinion shall be deemed a denial of the above-captioned application, on the grounds stated herein.


(5) Without my prior approval, the government may not submit additional briefing on the bases for my conclusion that I cannot grant this application in its present form. However, if the government continues to seek authority for the type of surveillance discussed at note 17 supra

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and accompanying text, its further submissions shall include an analysis of the extent to which such surveillance is directed at selector e-mail addresses, and the extent to which it is directed at e-mail addresses that send or receive communications that are acquired because they refer to a selector e-mail address.

Done and ordered this 3^d day of April, 2007 in Docket No. [REDACTED]


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] b(6) and b(7)(C)
I, [REDACTED] Clerk,
do hereby certify that this document
is a true and correct copy
of the original. [REDACTED] b(6) b(7)(C)

~~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

[REDACTED]

(S)

Docket Number: b(7)(E)

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

[REDACTED]

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] 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]
[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]
[REDACTED]
[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

~~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]). 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]
[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]

FISA (TS)

Constitute “Facilities” Under

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)



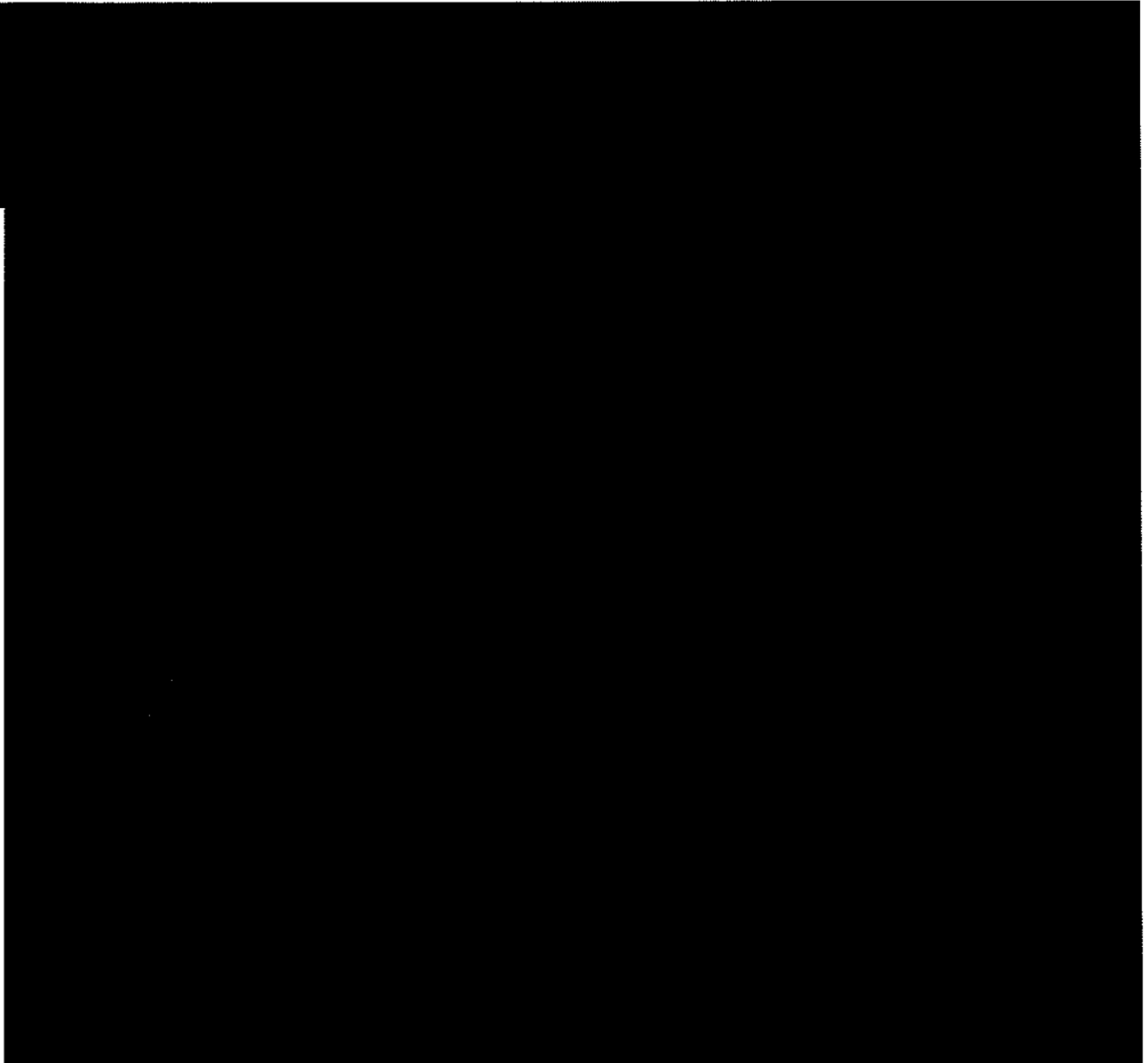
(TS//NF)

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)-

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

(S)-

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] 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] 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)

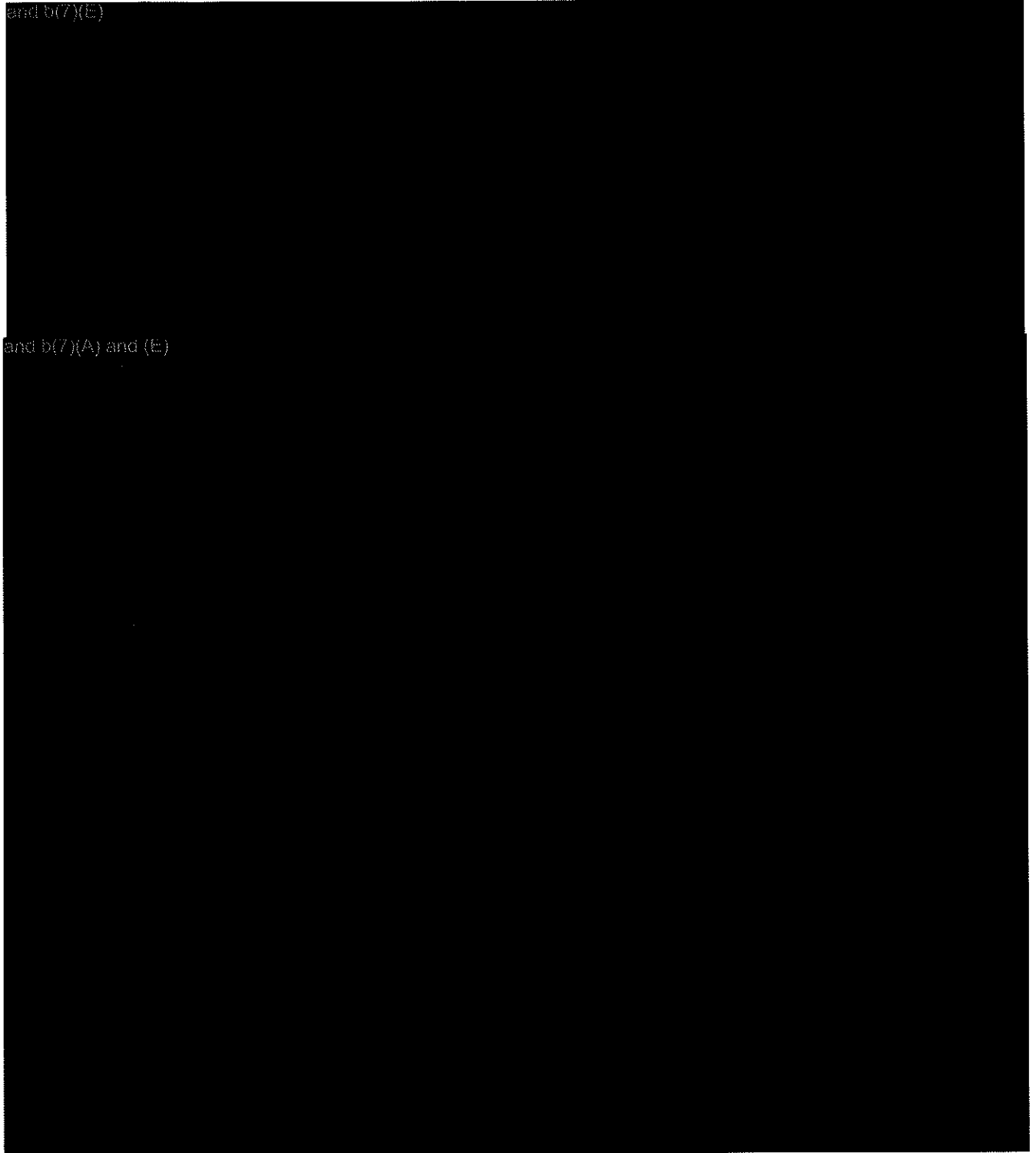
and b(6), b(7)(A), (C), and (E)



~~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.

~~(S)~~

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

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

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~~

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

APPROVED FOR PUBLIC RELEASE

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2007 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:

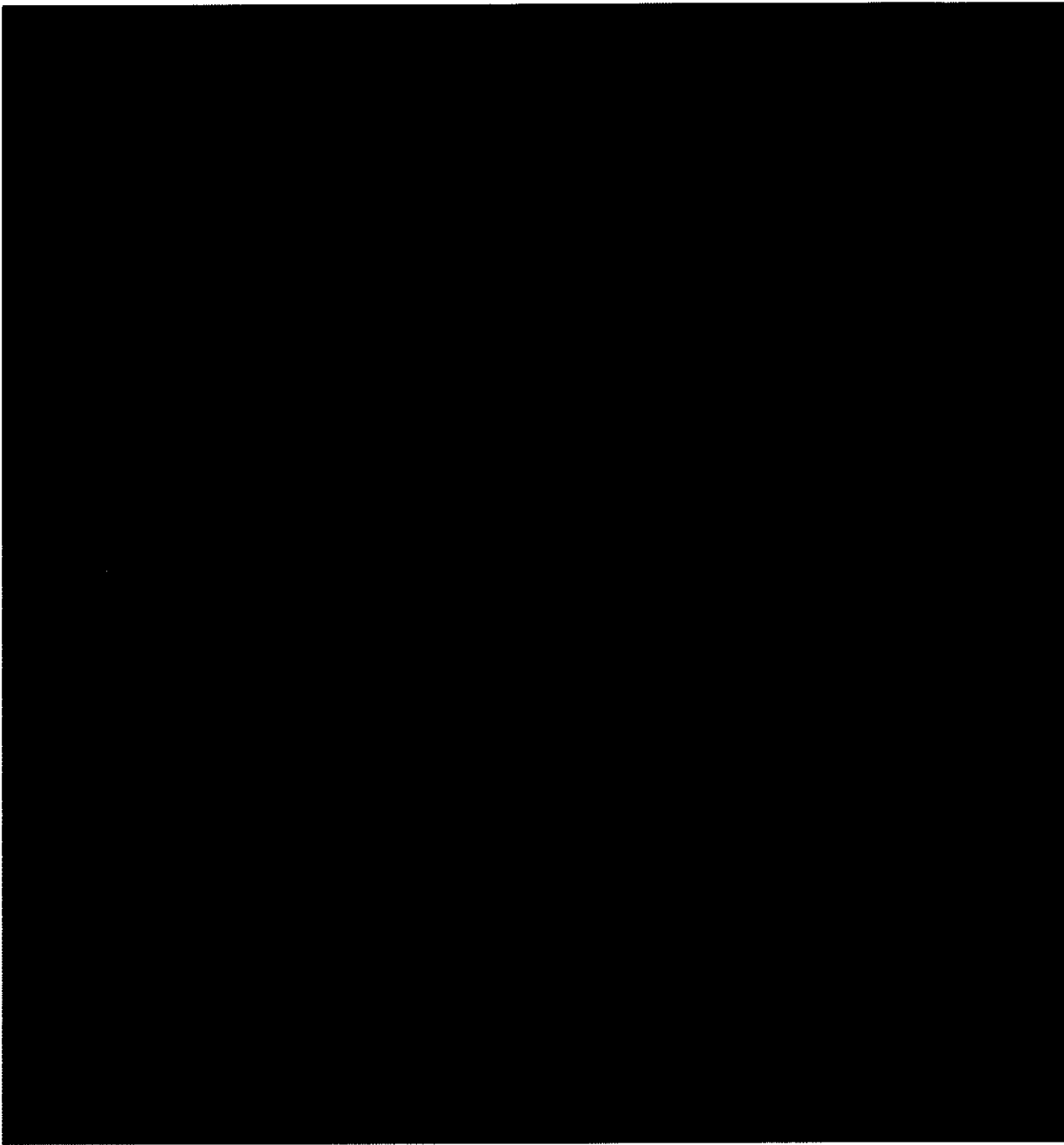
1. The President has authorized the Attorney General of the United States to approve applications for electronic surveillance for foreign intelligence information [50 U.S.C. § 1805(a)(1)];
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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

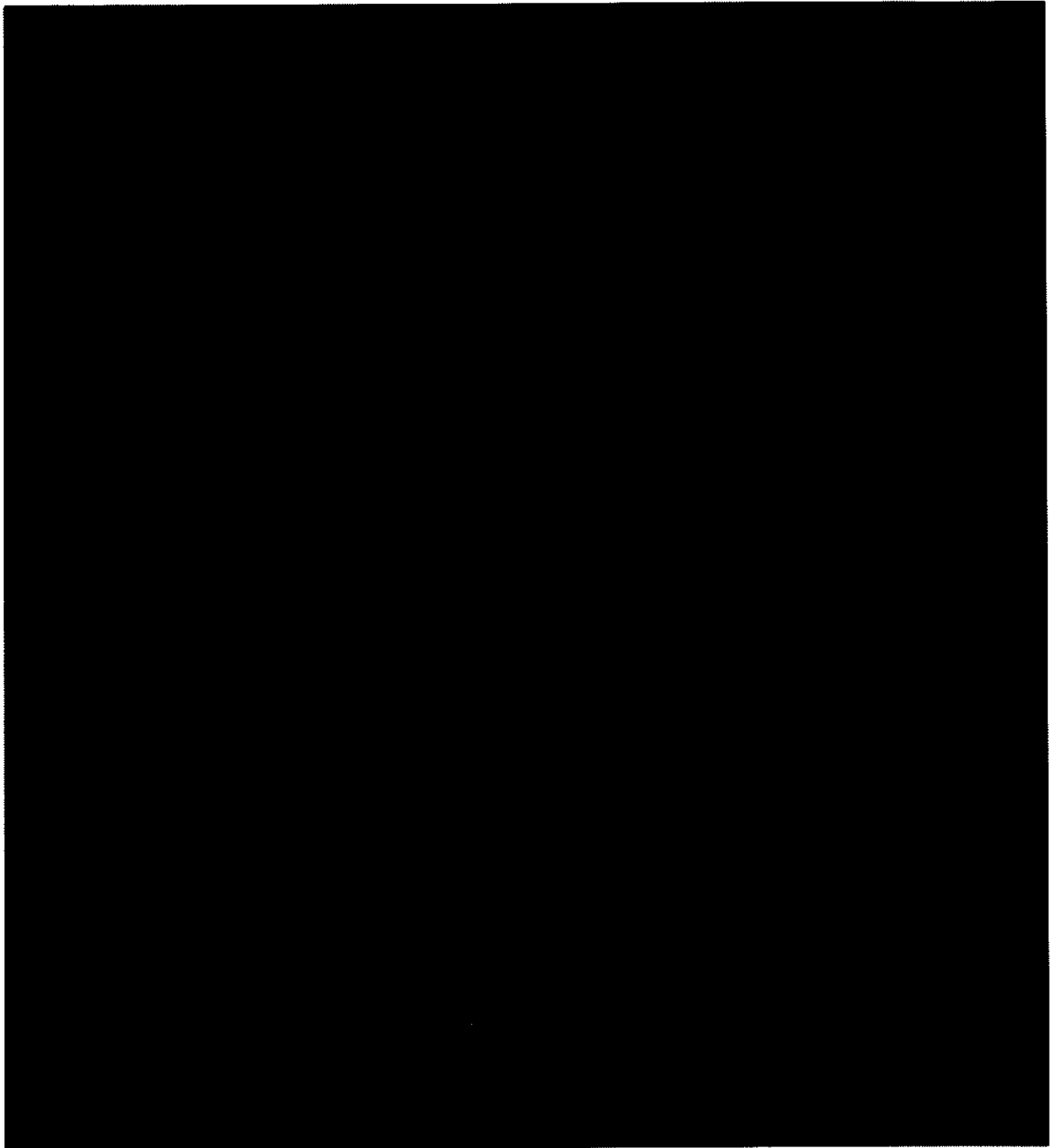
Derived from: Application to the USFISC in

~~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~~

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



1

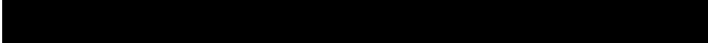


2



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

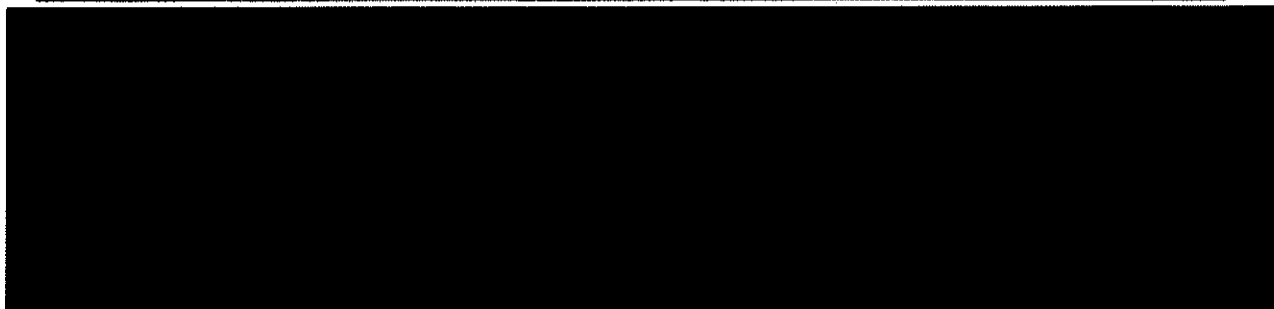
~~TOP SECRET//COMINT//NOFORN~~

(c) each of the facilities  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

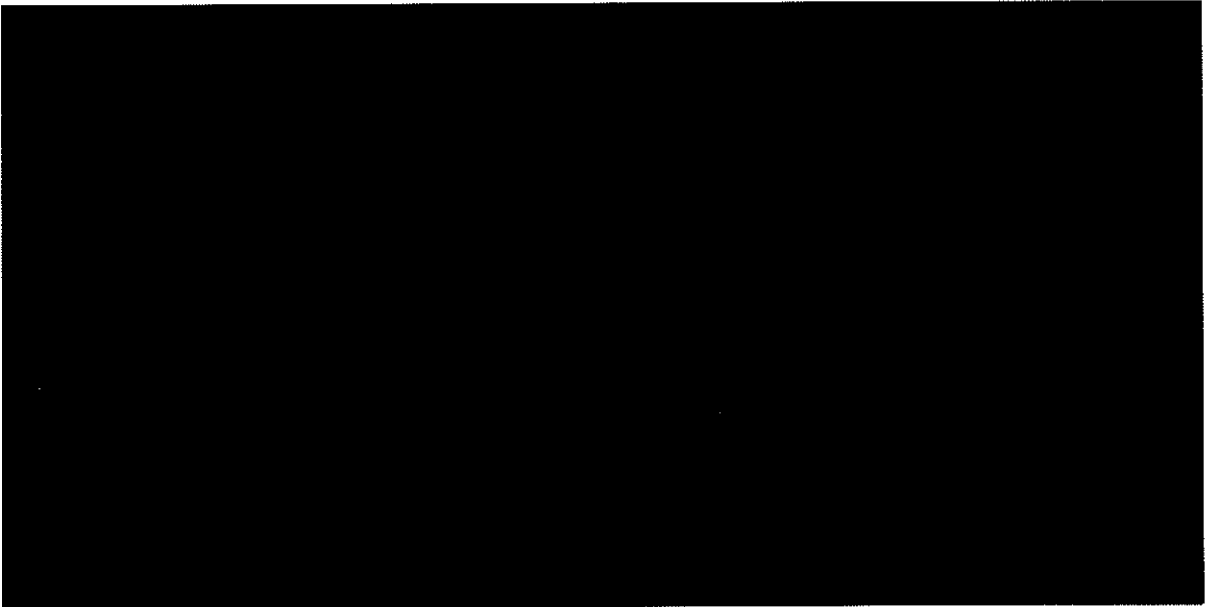


~~TOP SECRET//COMINT//NOFORN~~

~~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:



3



~~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]

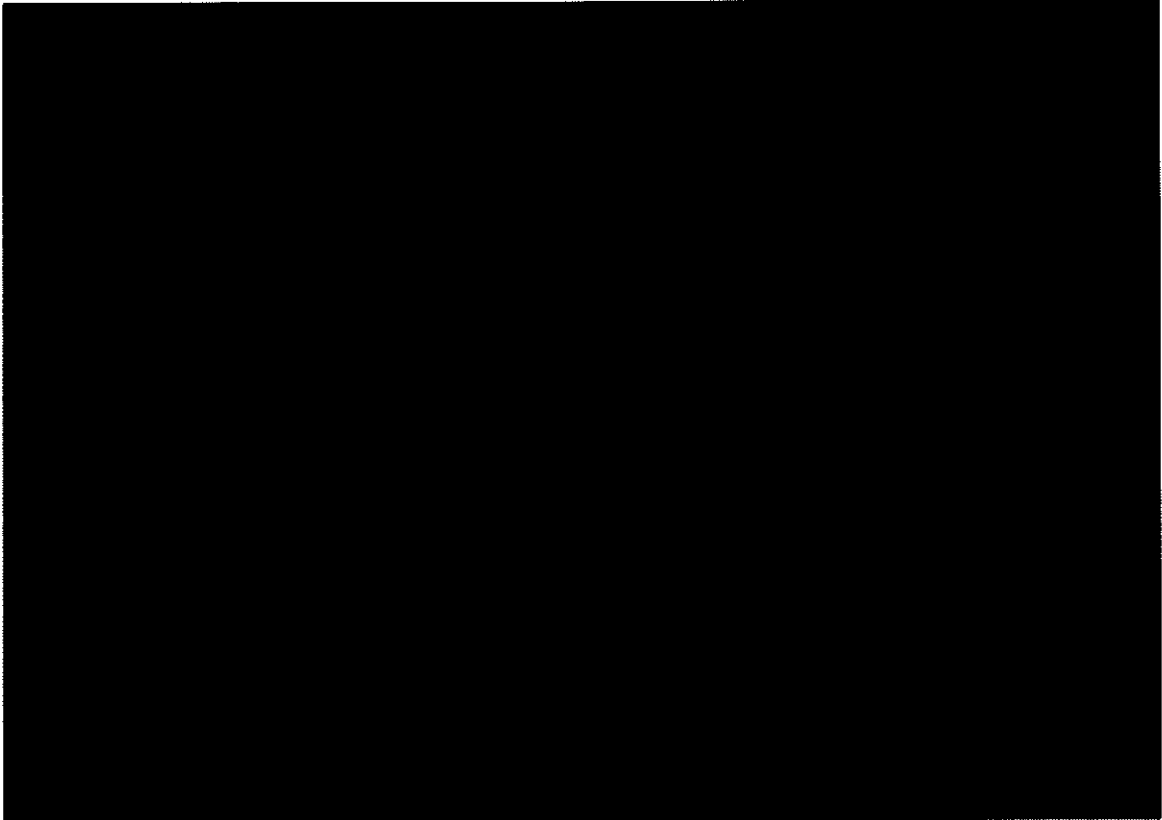
[REDACTED]

[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

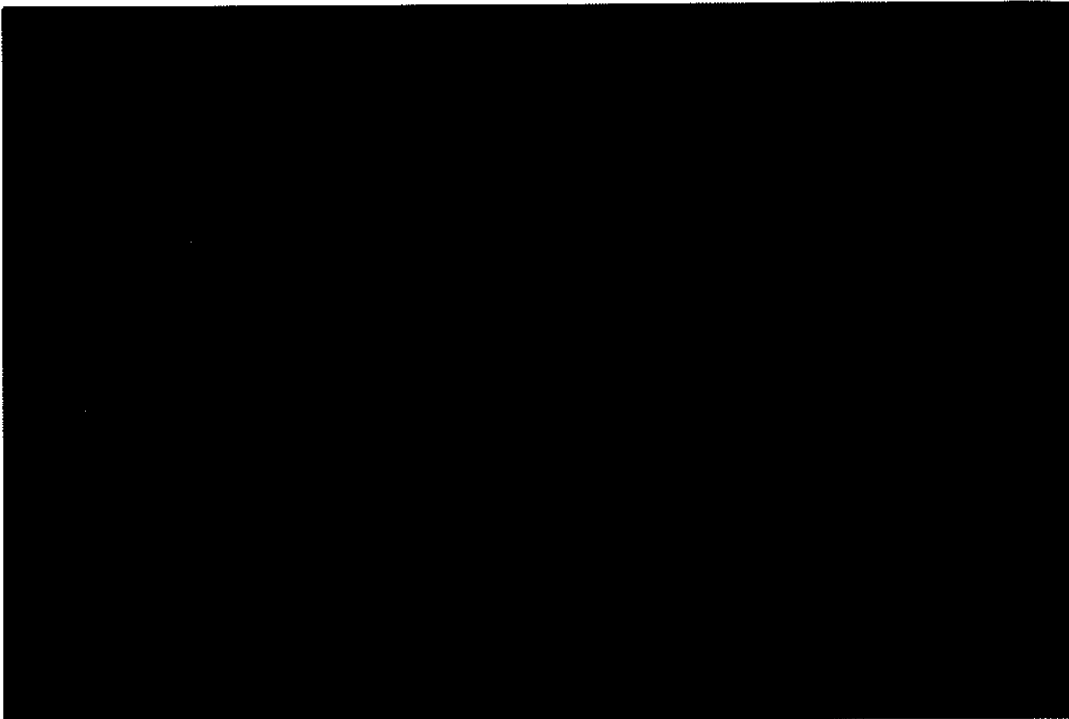


⁷

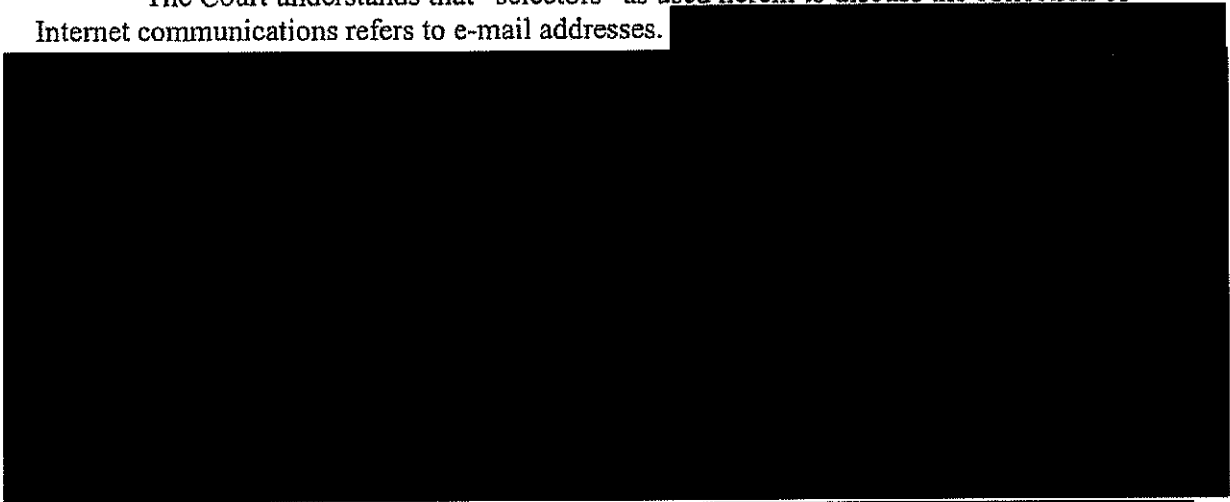


~~TOP SECRET//COMINT//NOFORN~~

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



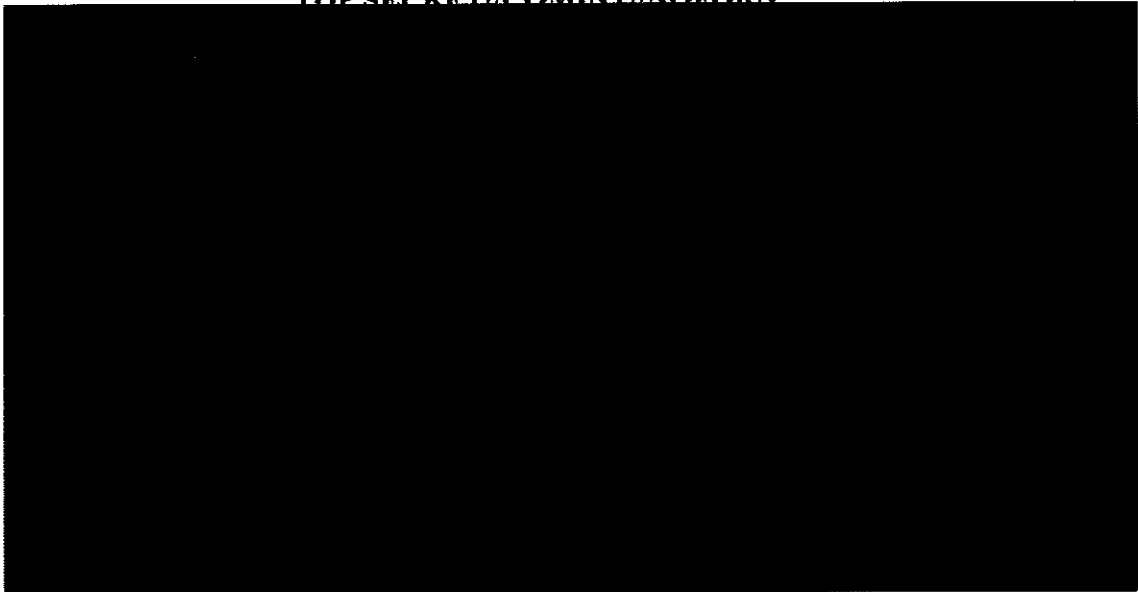
⁸ The Court understands that "selectors" as used herein to discuss the collection of Internet communications refers to e-mail addresses.



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.

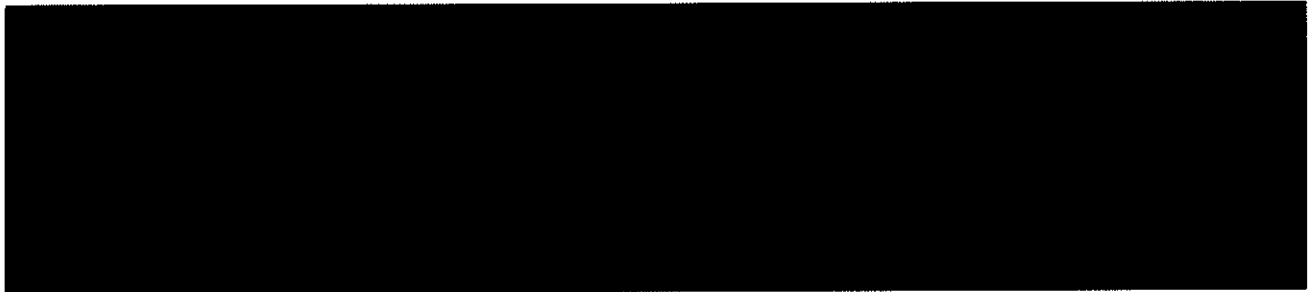
~~TOP SECRET//COMINT//NOFORN~~

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

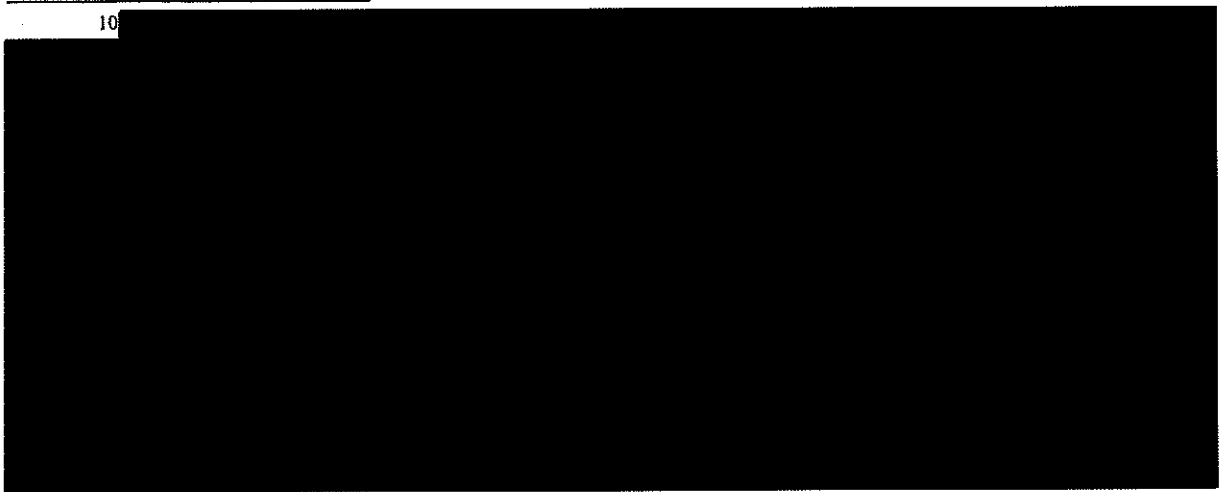


Unconsented physical entry is not authorized to implement the electronic surveillance approved herein.

(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.

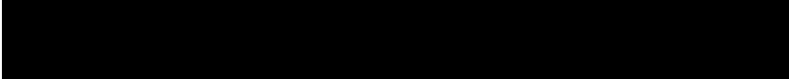
~~TOP SECRET//COMINT//NOFORN~~

~~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 

 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~~



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*86 Chambers Street
New York, New York 10007*

January 26, 2015

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: [REDACTED]@nytimes.com

Re: *The New York Times Co. v. U.S. Department of Justice*, 14 Civ. 3948 (VSB)

Dear David and Jeremy:

This Office represents the United States Department of Justice ("DOJ"), the defendant in the above-referenced matter. In accordance with the schedule set forth in the parties' joint submission on October 9, 2014, *see* Dkt. No. 11, as modified by the Court's December 8, 2014, order, *see* Dkt. No. 13, DOJ is releasing the enclosed documents in partial response to the Freedom of Information Act ("FOIA") request that is the subject of this litigation. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), (b)(6), (b)(7)(C), and (b)(7)(E). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

These documents also are being made available to the public on the Director of National Intelligence's website, "IC on the Record," at <http://icontherecord.tumblr.com/>, as well as at www.dni.gov.

If you have any questions, please do not hesitate to contact us.

Sincerely,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ John Clopper
JOHN D. CLOPPER
EMILY E. DAUGHTRY
ANDREW E. KRAUSE
Assistant United States Attorneys
Telephone: (212) [REDACTED]
Facsimile: (212) 6 [REDACTED]
E-mail: [REDACTED]@usdoj.gov
[REDACTED]@usdoj.gov
[REDACTED]@usdoj.gov

Enclosures

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

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



:

: Docket Number:



:

:

ORDER

On April 3, 2007, I entered an Order and Memorandum Opinion in the above-captioned docket number (April 3 Order), in response to the first application filed in the above-captioned docket number on March 21, 2007. The April 3 Order held that the proposed electronic surveillance was directed at individual telephone numbers and e-mail addresses, rather than the facilities

identified by the Government. *Id.* at 6-16. It also granted a motion by the Government for leave to file for an extension of the prior order, in Docket No. under which this surveillance was previously authorized. *Id.* at 20-21. Leave to

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

Derived from: Application to the USFISC in the
Docket Number captioned above

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

seek an extension was granted in order to "give the government a reasonable amount of time to work in good faith toward the preparation and submission of a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion." *Id.* at 21.

On April 5, 2007, the Government obtained from another judge of this Court an extension of the order in Docket No. [REDACTED]. Under that extension, current surveillance authorities expire at 5:00 p.m. on May 31, 2007.

The April 3 Order also required the Government to submit periodic reports regarding its efforts to prepare and submit a revised and supplemented application. In its report submitted on April 20, 2007, the Government articulated a new legal theory, under which it proposed that the Court would make probable cause findings for each telephone number and e-mail address identified at the time of the application as one at which surveillance would be directed, but that the Government could initiate electronic surveillance of later-discovered numbers and addresses, subject to reporting to the Court under 50 U.S.C. § 1805(c)(3).

On May 24, 2007, the Government filed a revised and supplemented application that seeks, *inter alia*, authority to conduct electronic surveillance of more than [REDACTED] identified telephone numbers and e-mail addresses and to initiate electronic

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

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

surveillance of later-discovered numbers and addresses on the theory noted above. On May 30, 2007, the Government submitted a Supplemental Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director of the National Security Agency (NSA), as well as a Declaration of (b)(3); (b)(6), NSA. Both the revised and supplemented application and the Supplemental Declaration filed on May 30 contain individual statements of the Government's factual basis for asserting probable cause to believe that each identified telephone number and e-mail address is being used, or about to be used, by one of the targeted foreign powers. I have reviewed each of these statements of facts, which were provided on a rolling basis prior to their formal submission. This Order addresses the revised and supplemented application, as further supplemented by the declarations filed on May 30, 2007, and by the Notice of Withdrawal, in Part, of Application for an Order Authorizing Electronic Surveillance filed on May 31, 2007 (the application). The Court continues to exercise jurisdiction over this matter for the reasons stated in the April 3 Order at page 8 n.12.

Having given full consideration to the matters set forth in the Government's application and all of the Government's other filings in this docket, as well as the hearings I have conducted with the Government, I find as follows:

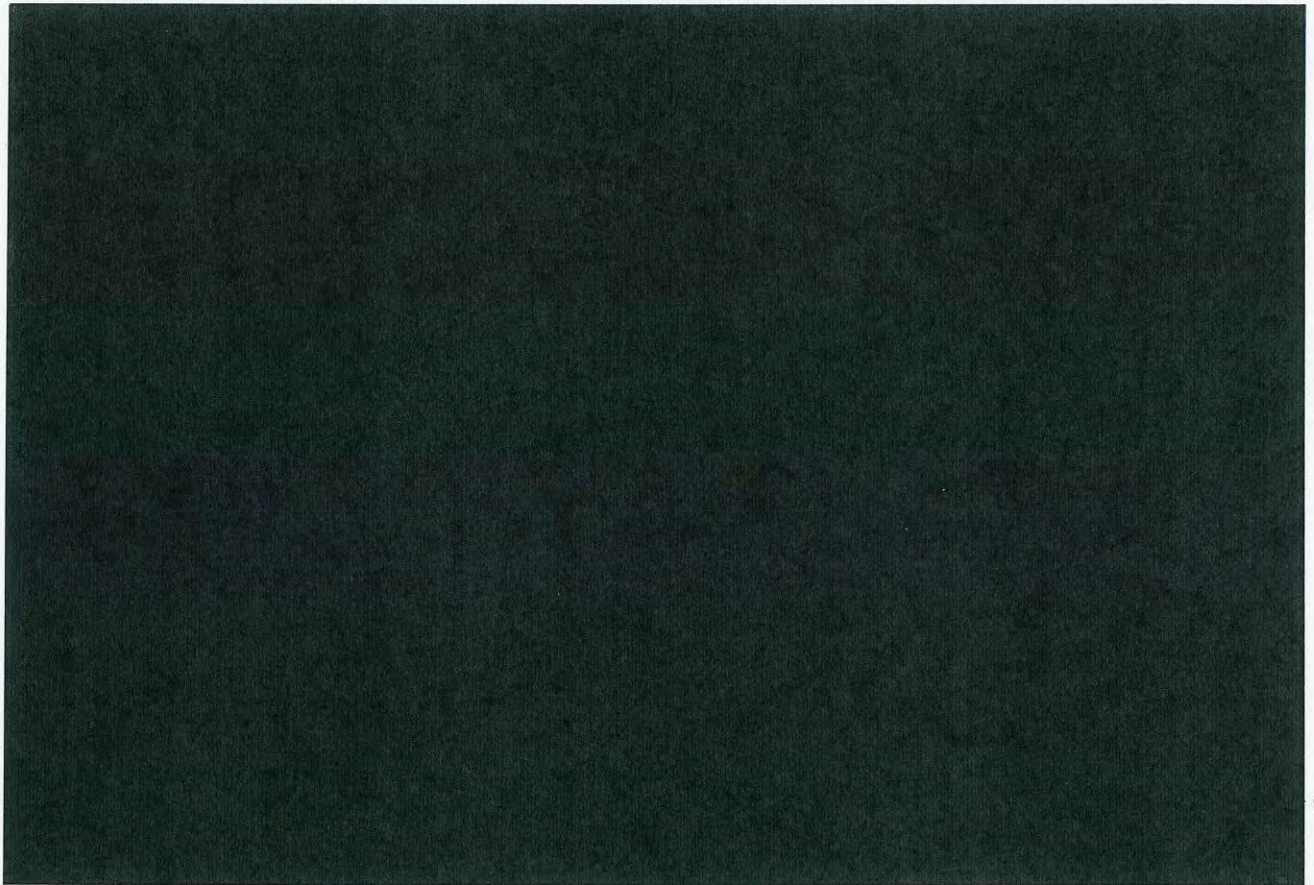
~~TOP SECRET//COMINT//NOFORN~~

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

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)];

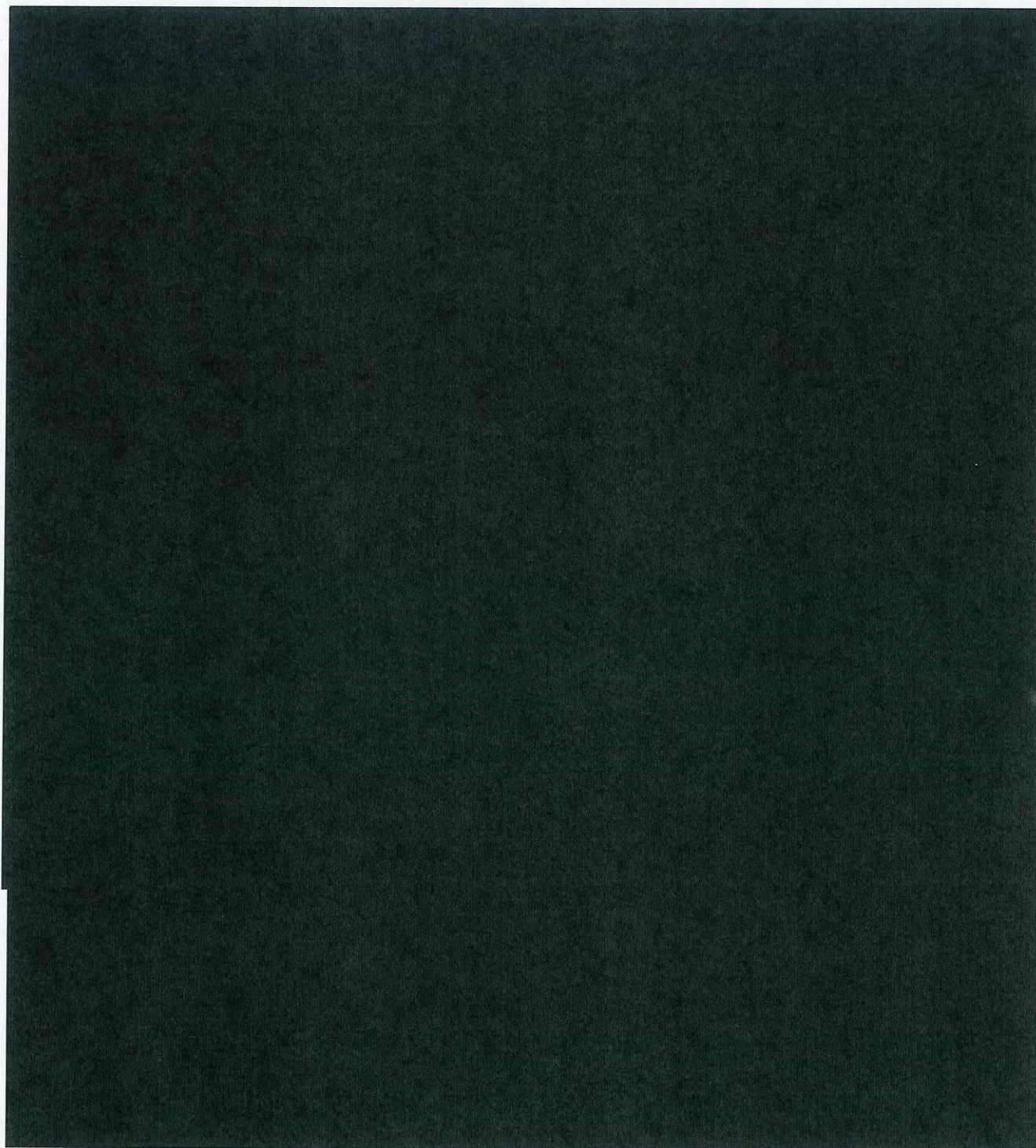
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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)];



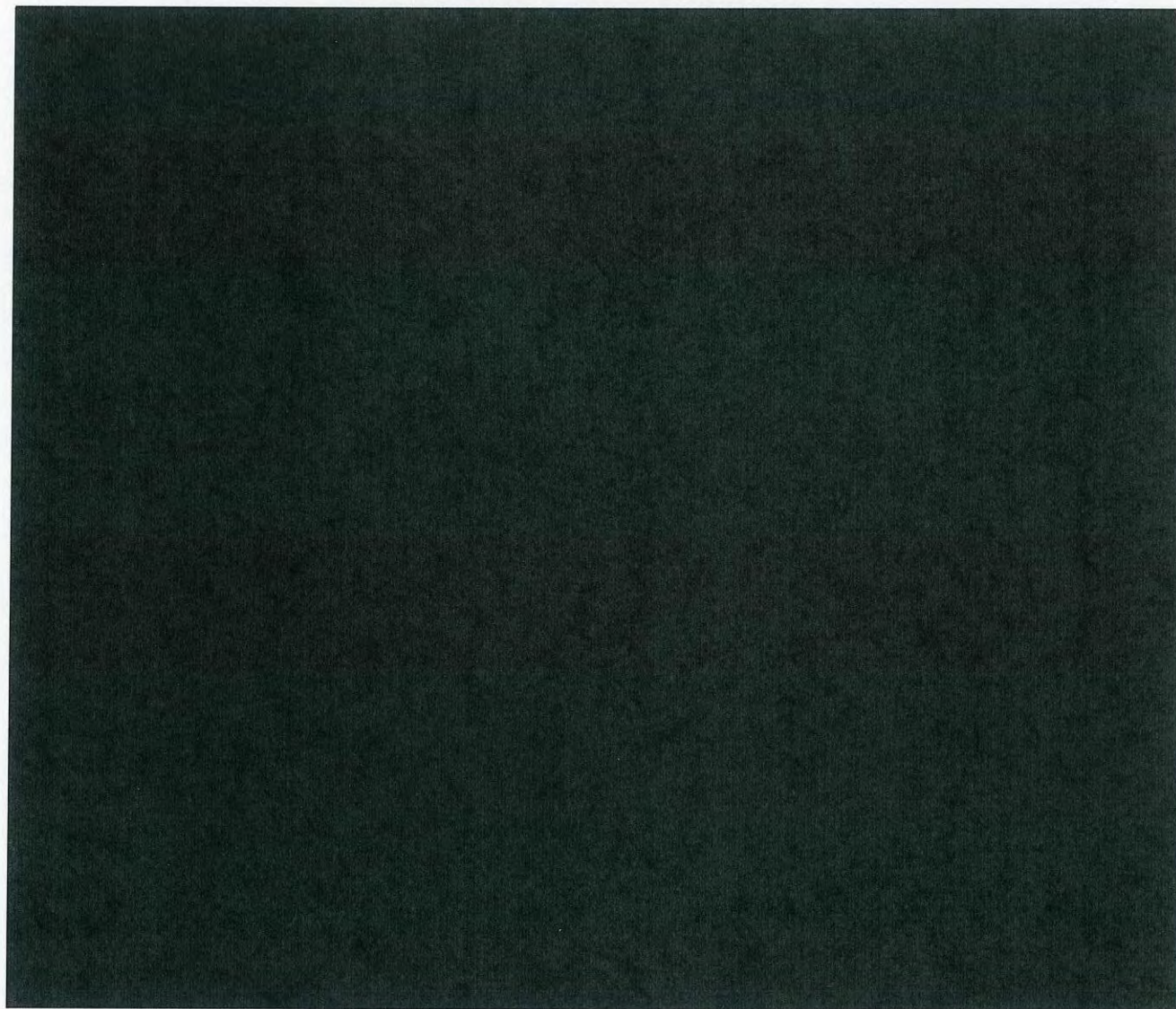
~~TOP SECRET//COMINT//NOFORN~~

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



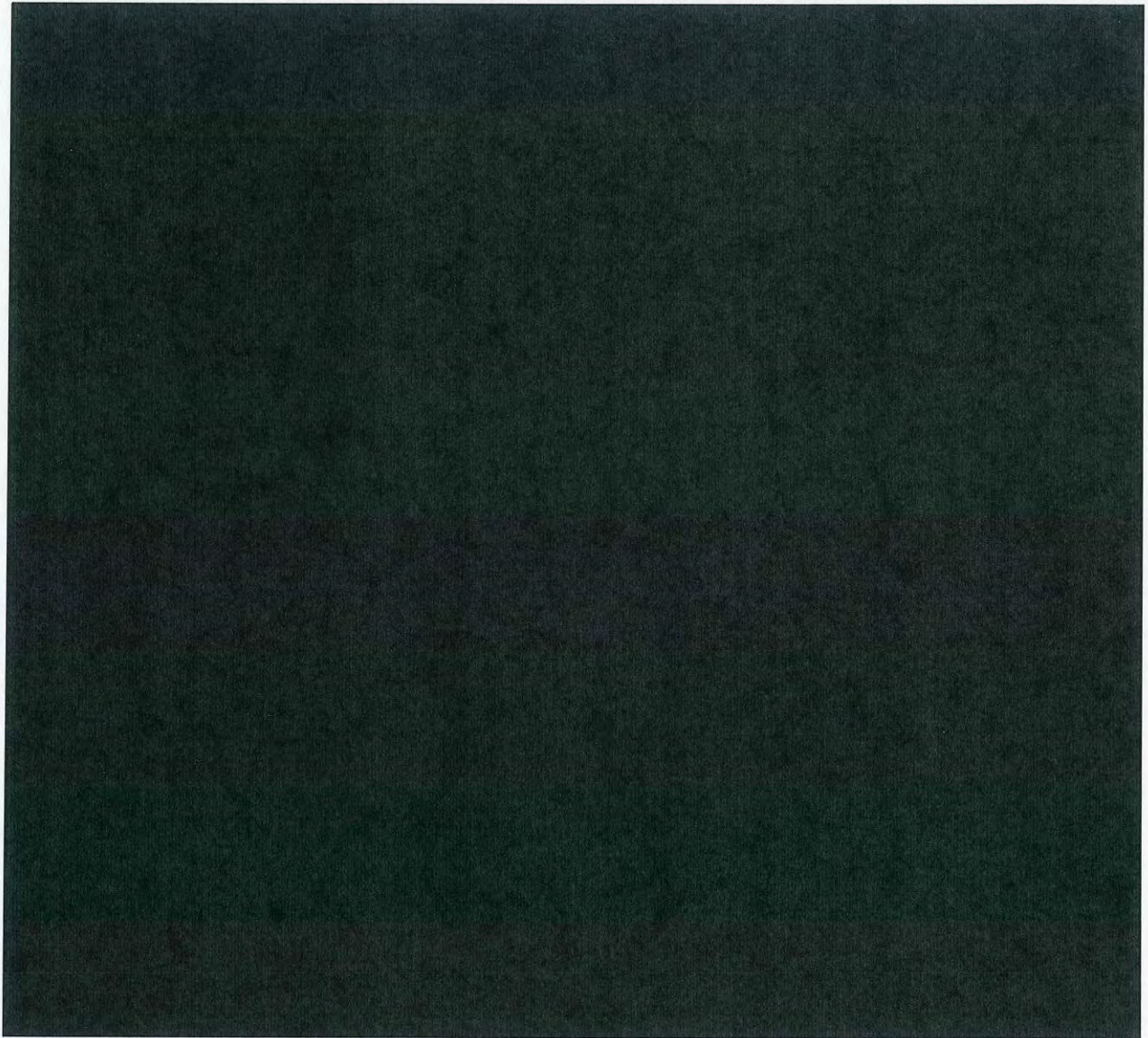
~~TOP SECRET//COMINT//NOFORN~~

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



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

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



2



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

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

(c) each of the facilities identified in Attachments A and B to Exhibit B in the revised and supplemented application, filed on May 24, 2007, and in Attachments A and B to the Supplemental Declaration of General Alexander, filed on May 30, 2007, but excluding the facilities identified in the Notice of Withdrawal filed on May 31, 2007, 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 paragraph II. below [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 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)].






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

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

WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States to conduct electronic surveillance, as described in the application, is GRANTED, and it is FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

I. The United States is authorized 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 described below, subject to the minimization procedures specified in paragraph 4 above and specifically detailed in paragraph IV below, for a period of ninety days, unless otherwise ordered by the Court.

(a). The facilities described in paragraph 3(c) above.

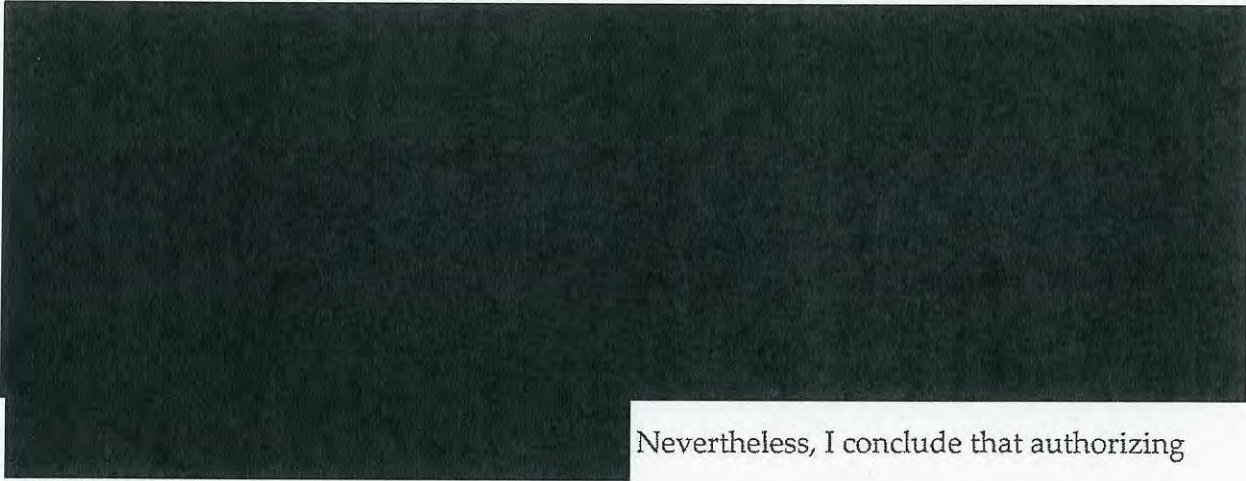
(b). It is well established that the targeted foreign powers pose a grave terrorist threat to the United States. ^{(b)(6); (b)(7)(C)} Declaration, at 10-12, 61-64. The evidence further establishes that the members and agents of the targeted foreign powers engage in a variety of activities in order to thwart or counter surveillance, 



Id., at 89, 94-98.

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

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

While the provisions of 50 U.S.C. § 1805 are in tension with one another,³ it appears that the intent of Congress, when amending these provisions in 2001 and 2006, was to authorize multipoint or "roving" surveillance of a target that is actively avoiding surveillance, and to provide judicial oversight of such surveillance through the notice requirement in 50 U.S.C. § 1805(c)(3).⁴ This Court's practice has generally been to



Nevertheless, I conclude that authorizing

³ On the one hand, 50 U.S.C. § 1805(a)(3)(B) requires that the judge find probable cause to believe that each of the facilities at which surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. On the other hand, 50 U.S.C. § 1805(c)(1)(B) clearly envisions cases in which the Court's order would authorize electronic surveillance of facilities, under circumstances where the nature and location of the facilities were unknown at the time the application was approved. Similarly, the notice requirement in 50 U.S.C. § 1805(c)(3) indicates that an order can, consistent with 50 U.S.C. § 1805(c)(1)(B), authorize electronic surveillance of "any new facility or place," and suggests that the order can authorize the government to determine whether "each new facility or place" is being used, or is about to be used, by the target of surveillance, subject to prompt notice to, and review by, this Court.

⁴ The legislative history for the USA PATRIOT Act's amendment to § 1805(c)(2)(B) states that the new language was "included... to modify [FISA] to allow surveillance to follow a person who uses multiple communications devices or locations, a modification which conforms FISA to the parallel criminal procedures for electronic surveillance in 18 U.S.C. § 2518(1)(b)." 147 Cong. Rec. S11006 (Daily ed. Oct. 25, 2001) (section-by-section analysis of Sen. Leahy). The subsequent addition of "if known" to § 1805(c)(1)(B) was intended "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." H.R. Conf. Rep. No. 107-328, at 24 (2001). The notice requirements set forth in § 1805(c)(3) were added in 2006 by section 108(b)(4) of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177, to add "an extra layer of judicial review and to ensure that intelligence investigators will not abuse the multipoint authority." Conf. Rep. H.R. 3199, reprinted in Cong. Rec. at H11303.

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

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

such surveillance in this case is consistent with the provisions of 50 U.S.C. § 1805, as well as the intent of Congress, and is particularly appropriate where, as is the case here, the national security interests of the Government are great, and the impact of the surveillance on the Constitutional rights of United States persons is, or can be, minimized.

Therefore, in accordance with 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3), the United States is authorized to conduct electronic surveillance of any other telephone numbers or e-mail [REDACTED] the nature and location of which are not specified herein because they were unknown to the NSA as of May 24, 2007 (the date the application was filed), where there is probable cause to believe that each additional telephone number or e-mail [REDACTED] is being used, or is about to be used, [REDACTED]

[REDACTED] This authority shall be limited to the surveillance of telephone numbers and e-mail [REDACTED] which the NSA reasonably believes are being used, or about to be used, by persons outside the United States and shall not include the surveillance of telephone numbers and e-mail [REDACTED] that the

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

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

NSA reasonably believes are being used, or about to be used, by United States persons, as defined in 50 U.S.C. § 1801(i).

(c). In this case, the Government has also asked for specific authority to acquire certain electronic communications that relate to or refer to an e-mail

[REDACTED] that is targeted for surveillance under this Order. For example, the Government argues that it should be allowed to acquire any e-mail communication that mentions a targeted e-mail [REDACTED] even though the communication is to and from other e-mail [REDACTED] not currently under electronic surveillance.⁵ After careful consideration of the Government's arguments, the Court holds that, in the limited and carefully considered circumstances described below, there is probable cause to believe that internet communications relating to a previously targeted e-mail [REDACTED] are themselves being sent and/or received by one of the targeted foreign powers, and thus those communications may be acquired by the NSA. At the same time, any e-mail facilities that were involved in sending or receiving such communications may not be further targeted absent a further examination by the NSA of the evidence supporting probable cause that involves, among other things, looking at the actual content of the

⁵ The Government identifies these as "abouts" or "referred to" communications. "For example, if an unknown [REDACTED]

Memorandum of Law at 4.

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

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

original intercepted communication which refers to the previously targeted e-mail

[REDACTED] This holding, albeit novel, is consistent with the overall statutory requirements; it requires the Government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers. This Court will be able to ultimately determine whether the electronic surveillance was proper.

Therefore, in accordance with 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3), the United States is further authorized to conduct electronic surveillance, as follows:

(i) by acquiring internet communications that contain a reference to an e-mail

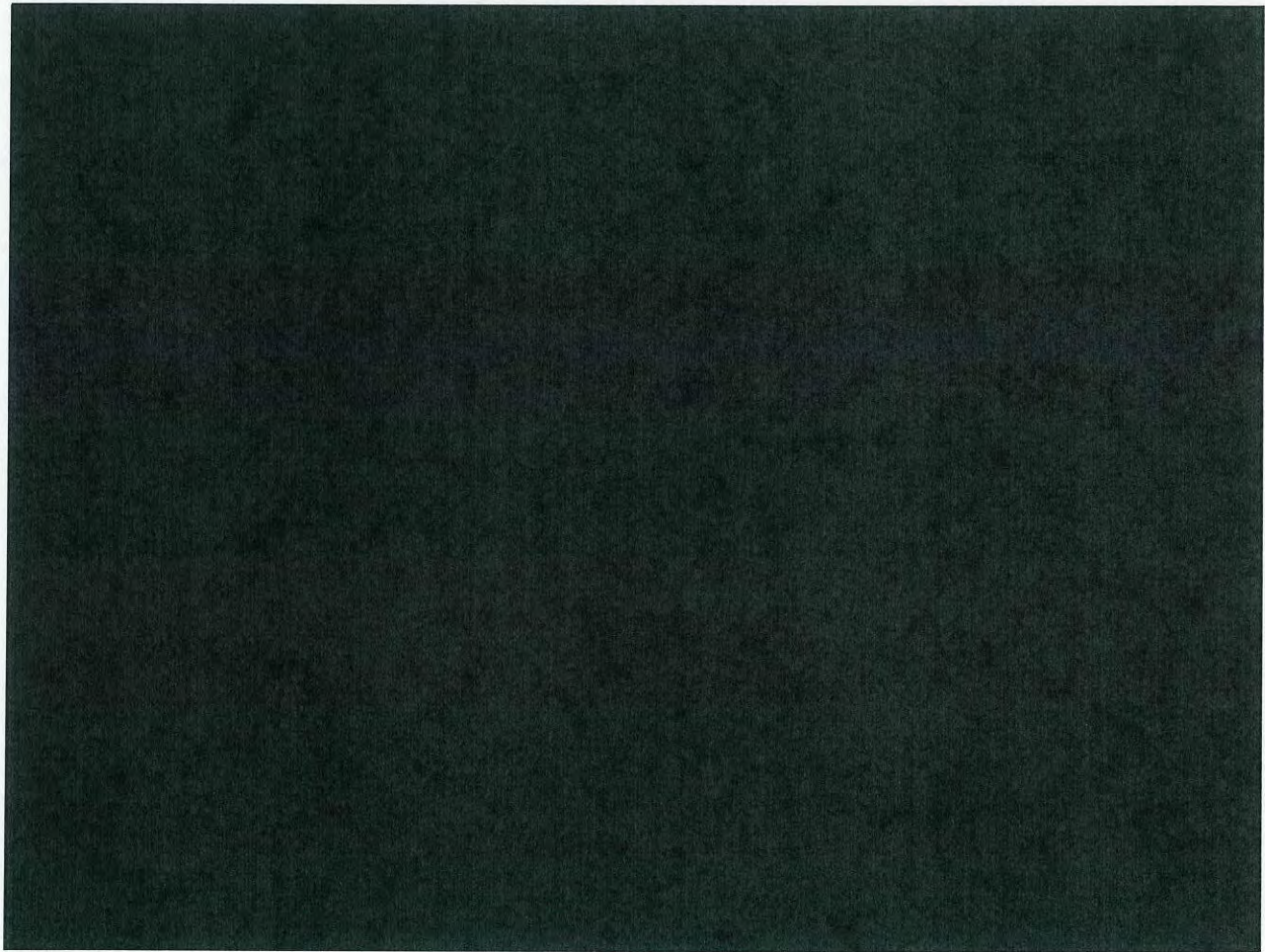
[REDACTED] that is subject to electronic surveillance under this Order at the time of acquisition (targeted [REDACTED]), under one of the following circumstances:

⁶ For example, if the user of targeted [REDACTED]

[REDACTED] account under this authority. The government's application does not ask separately for authority to initiate electronic surveillance under these circumstances, Memorandum of Law, at 2, apparently on the theory that [REDACTED] is actually electronic surveillance directed at the already targeted [REDACTED]. However, I conclude that electronic surveillance is directed at the newly identified facility in cases where that facility is separate and distinct from the already targeted [REDACTED]

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

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



[redacted] Therefore, separate authority is required to direct this form of electronic surveillance at a new facility, i.e., a separate [redacted] and I grant such authority here.

⁷ For purposes of this Order, [redacted]

⁸ For example, if the user [redacted]

[redacted] See Memorandum of Law, at 3. The government's application does not ask separately for authority to initiate electronic surveillance of [redacted] under these circumstances. *Id.*, at 2. However, for the same reasons discussed in footnote 6, it seems to me that separate authority is required to initiate electronic surveillance of a separate facility, [redacted] and I grant such authority here.

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

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

I conclude and find that in each of the circumstances described [REDACTED]

[REDACTED] above, there is probable cause to believe that the facility at which electronic surveillance is directed is being used, or is about to be used, by [REDACTED]

[REDACTED] and

(ii) by targeting for collection by means of internet communications surveillance, as defined in paragraph II. below, an e-mail [REDACTED] a communication of which has been acquired pursuant to clause (i) above, only when all of the following requirements are satisfied:

(A). the NSA determines, on the basis of the contents of the acquired communication, and other reliable intelligence or publicly available information, there is still probable cause to believe that the e-mail [REDACTED] is being used, or is about to be used, by one of the targeted foreign powers;

(B). the NSA reasonably believes that the e-mail [REDACTED] is being used, or is about to be used, by persons outside the United States; and

(C). the NSA does not have reason to believe that the e-mail [REDACTED] is being used, or is about to be used, by a United States person, as defined in 50 U.S.C. § 1801(i).

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

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

For each new facility at which the Government directs electronic surveillance under sub-paragraphs (b) or (c)(ii) above, the Government shall provide notice to the Court in accordance with 50 U.S.C. § 1805(c)(3) within twenty-one days after the date on which such surveillance begins and in accordance with the following reporting schedule. The first such report shall be filed on Wednesday, June 13, 2007; this first report shall provide notice of newly discovered telephone numbers and e-mail [REDACTED] for which the Government initiated electronic surveillance from May 24, 2007 (i.e., the date on which this application was filed) through June 2, 2007. Subsequent reports shall be filed on a weekly basis each Wednesday (or on Tuesday if Wednesday is a national holiday), and will cover surveillance initiated during an earlier one-week period. For example, on June 20, 2007, the Government shall provide a report on surveillance initiated from June 3, 2007, through June 10, 2007; on June 27, 2007, the Government shall provide a report on surveillance initiated from June 11, 2007, through June 18, 2007; and so on. Such notice shall include:

- (A) the nature and location of each new facility or place at which electronic surveillance is directed;
- (B) the facts and circumstances relied upon by the United States to justify its belief that the new facility or place at which the electronic surveillance is directed

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

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

is or was being used, or is about to be used, by a target of surveillance (for surveillance conducted pursuant to paragraph I(c)(ii), the notice shall include the facts and circumstances relied upon by the United States to justify its continued surveillance of that facility);

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of this Order.

In accordance with 50 U.S.C. § 1805(c)(3), I find that the Government has established good cause to justify the twenty-one day period described above.

In addition, for each new facility at which the Government directs electronic surveillance under sub-paragraph (c)(i) above, the Government shall provide notice to the Court in accordance with 50 U.S.C. § 1805(c)(3) within sixty days after the date on which such surveillance begins and in accordance with the following reporting schedule. The first such report shall be filed on Wednesday, July 30, 2007; this first report shall provide notice of each new facility for which the Government initiated electronic surveillance from May 31, 2007 (i.e., the date of this Order) through July 15, 2007. The second report shall be filed fifteen days after the expiration of this Order, and shall provide notice of each new facility for which the Government initiated electronic

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

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

surveillance from July 16, 2007 through the expiration of the authorized surveillance.

Such notice shall include:

- (A) the nature and location of each new facility or place at which electronic surveillance is directed;
- (B) the facts and circumstances relied upon by the United States to justify its belief that the new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by a target of surveillance;
- (C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
- (D) the total number of electronic surveillances that have been or are being conducted under the authority of this Order.

In accordance with 50 U.S.C. § 1805(c)(3), I find that the Government has established good cause to justify the sixty day period described above.

The Court may order the Government to immediately cease electronic surveillance of any facility as to which it deems the facts and circumstances relied upon by the Government to be inadequate.

In addition, the Government shall continue to file emergency FISA applications pursuant to 50 U.S.C. § 1805(f)(or alternatively, a motion to amend) if it seeks authority to conduct electronic surveillance, as described herein, of additional telephone numbers and e-mail [REDACTED] that the Government believes are being used,

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

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

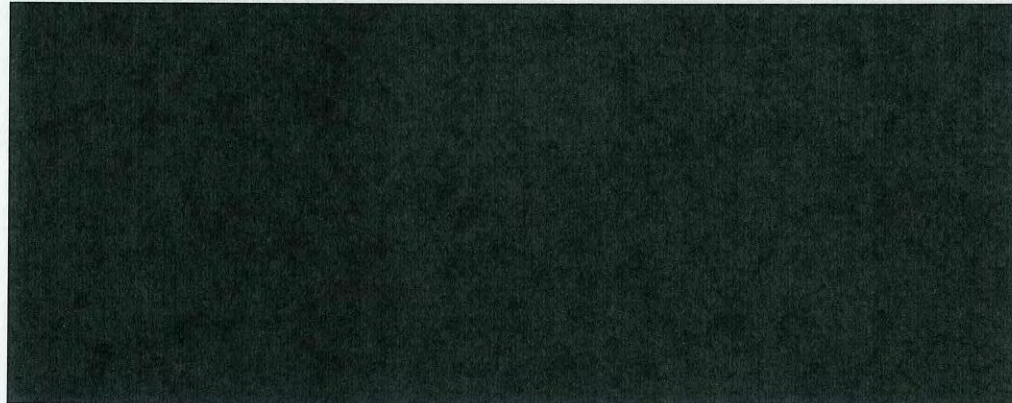
or are about to be used, by one of the targeted foreign powers and which are reasonably believed to be used by persons located outside the United States who are United States persons as defined in 50 U.S.C. § 1801(i). The Government has proposed a streamlined FISA emergency application form, attached as Exhibit G to the application, specifically for this purpose. I find that for any such application made under the above-captioned docket number the form of this proposed application is consistent with FISA.

I also hereby find that the Government has established "good cause" within the meaning of 50 U.S.C. § 1806(j) that a subject of emergency surveillance initiated by the Government during the period of this Order, but not authorized by this Court, should not be notified of the emergency employment of electronic surveillance. For any such surveillance, the requirement of notice shall be suspended for ninety days following the emergency employment of electronic surveillance, provided that on a further ex parte showing of good cause by the Government, the Court shall forego ordering the serving of the notice required under section 50 U.S.C. § 1806(j).

II. The means by which this electronic surveillance shall be effected are as follows:

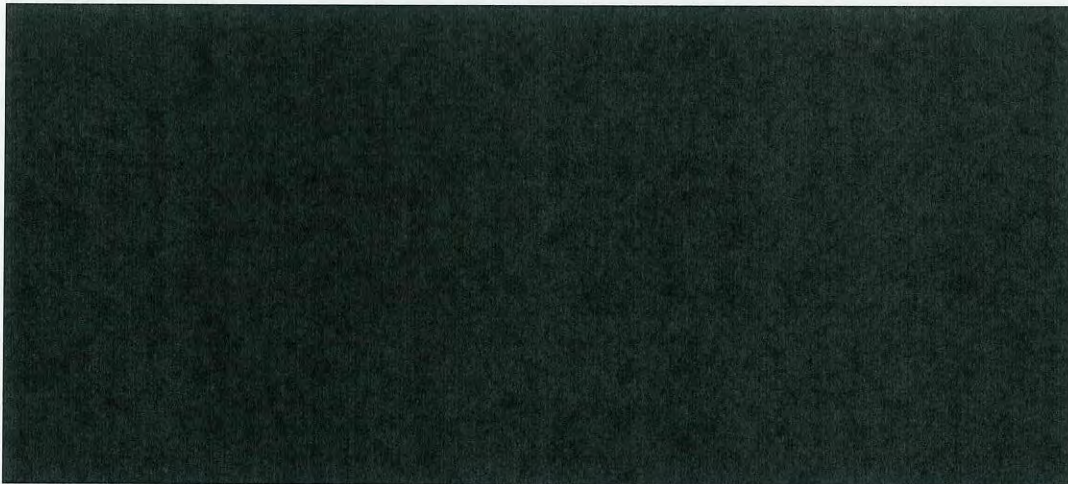
~~TOP SECRET//COMINT//NOFORN~~

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



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

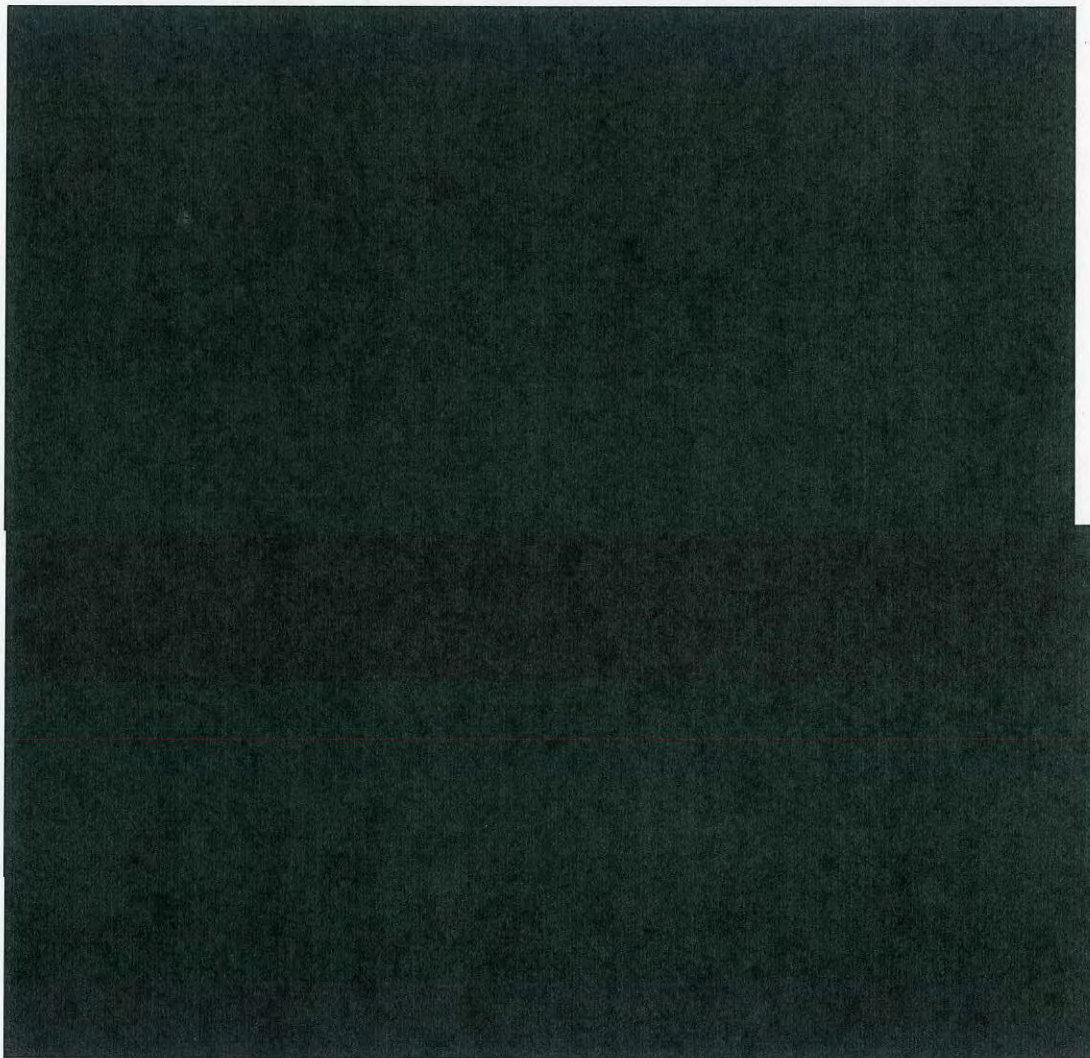
~~TOP SECRET//COMINT//NOFORN~~



¹¹ This Order is based on the principle that the NSA surveillance will be designed to acquire only international communications where a communicant is located outside the United States, but the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that no domestic communications will be acquired. 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~~



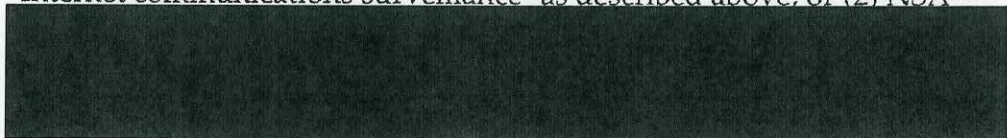
§1801(f)(4) surveillance. This surveillance will be effected by using either, or both, of two techniques, as follows: (1) The first technique constitutes



TOP SECRET//COMINT//NOFORN

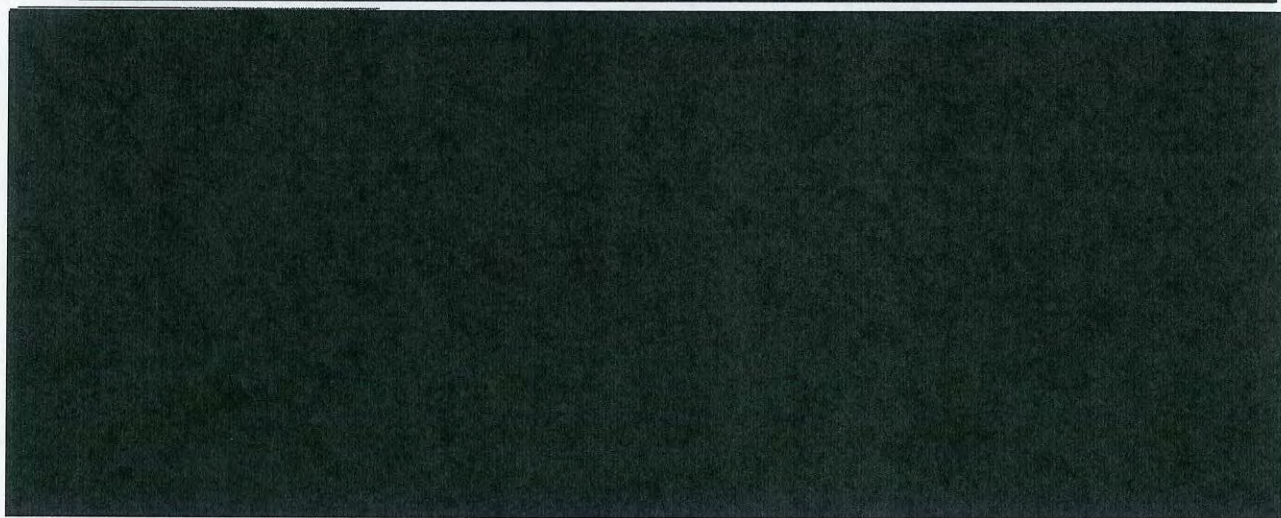
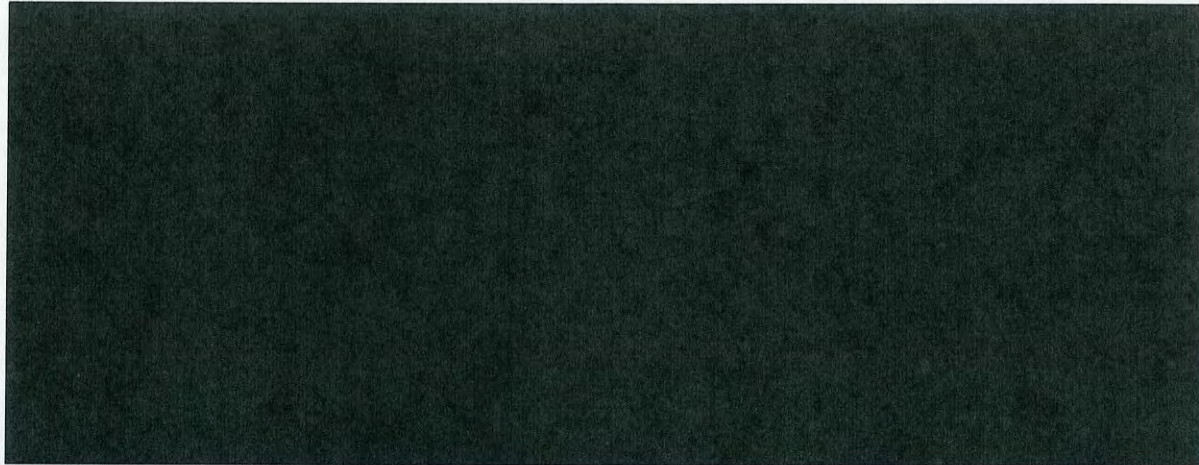
~~TOP SECRET//COMINT//NOFORN~~

"Internet communications surveillance" as described above; or (2) NSA



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

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



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

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

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, 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)].

IV. As to all information gathered through the authorities requested herein, the NSA shall follow:

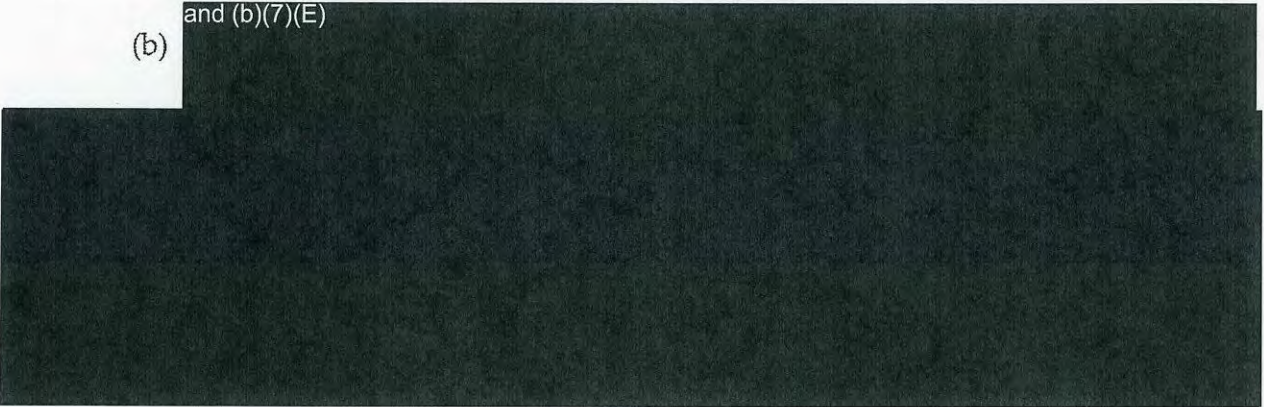
(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States

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

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

Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

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



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

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

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

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:¹⁴

(1) Disseminations to [REDACTED]

[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

14

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

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

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. 12333 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. 12333, 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.

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.

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

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

(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 B to the application.

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~~


V. The CIA shall minimize all communications received under this order as provided in Exhibit E to the application.

Signed 05-31-2007 10:15A Eastern Time
Date Time

This authorization regarding [REDACTED]

[REDACTED] expires at 5:00 p.m.

on the 24th day of August, 2007.



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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

(b)(6); (b)(7)(C)

Deputy Cler.

FISC, certify that this document
is a true and correct copy of
the original (b)(6); (b)(7)(C)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

:
:
:
:

Docket No.:



ORDER AND MEMORANDUM OPINION

This matter is before the Court on the Motion to Amend filed by the government in the above-captioned docket on July 27, 2007.

This motion concerns just one of the difficult issues presented by this effort to apply FISA to a complex, large-scale surveillance program. This case has required, and continues to require, an extraordinary expenditure of time and effort by NSA, the Department of Justice, and this Court, notwithstanding that it concerns electronic surveillance that is overwhelmingly directed at non-U.S. persons operating outside of the United States. In my view (a view I believe to be shared by all of the judges of this Court), legislative action is urgently needed to refocus the FISA process on surveillances that – unlike this one – significantly involve interests protected by the Fourth Amendment.

Background

This order is intended to clarify and supplement the earlier orders entered in this docket on April 3, 2007, and May 31, 2007. The May 31 order authorized electronic surveillance of particular, identified telephone numbers and e-mail addresses, on the basis of my finding probable cause to believe that such numbers and addresses were being or about to be used by one of the targets. May 31, 2007 Order at 8-9. It established procedures that were novel and were designed to meet the complex requirements of insuring that the requested surveillance by the NSA complied with the statutory provisions of FISA. That order also provided for adding additional numbers or addresses:

in accordance with 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3), the United States is authorized to conduct electronic surveillance of any other telephone numbers or e-mail [redacted] the nature and location of which are not specified herein because they were unknown to the NSA as of May 24, 2007 (the date the application was filed), where there is probable cause to believe that each additional telephone number or e-mail [redacted] is being used, or is

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

about to be used, by [one of the targeted foreign powers]. This authority shall be limited to the surveillance of telephone numbers and e-mail [REDACTED] which the NSA reasonably believes are being used, or about to be used, by persons outside of the United States and shall not include the surveillance of telephone numbers and e-mail [REDACTED] that the NSA reasonably believes are being used, or about to be used, by U.S. persons, as defined in 50 U.S.C. § 1801(i).

Id. at 11-12 (emphasis added). That order also established a schedule for the government to submit, pursuant to 50 U.S.C. § 1805(c)(3), weekly reports on the initiation of electronic surveillance of such additional facilities. Id. at 16-17.

Upon reviewing these reports, several judges of this Court have ordered supplementation with regard to whether NSA had knowledge prior to May 24, 2007, that would call into question whether it properly invoked the above-quoted provision of the May 31 Order.¹ The pending motion seeks clarification of what it means, under that provision, for the “nature and location” of a facility to have been “unknown to the NSA as of May 24, 2007.” I conducted a hearing on this motion on the record on August 2, 2007.

Discussion

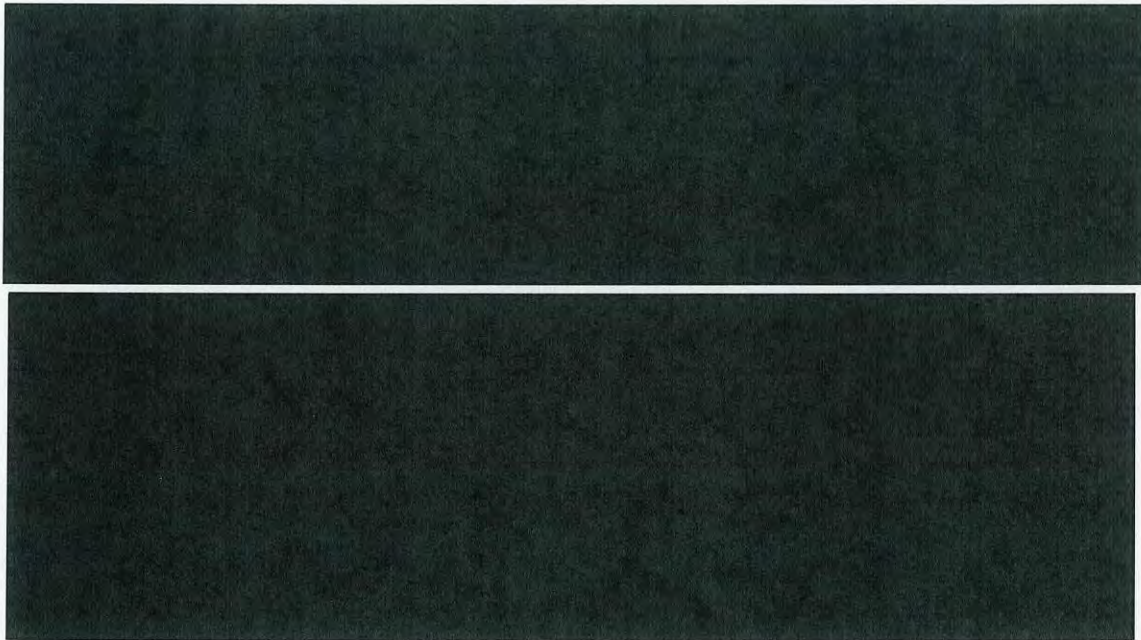
With the benefit of some two months of implementation, it can be seen that this provision of the May 31 Order requires clarification. As stated in the motion, and further addressed at the hearing, NSA has encountered different situations in which it has found the proper interpretation of this provision to be uncertain. The following hypothetical examples illustrate some of these concerns:



¹ See No. [REDACTED] Orders Dated June 22, 2007 (J. Kazen); July 6, 2007 (J. Bates); July 6, 2007 (J. Benson); July 13, 2007 (J. Scullin); July 20, 2007 (J. Kollar-Kotelly). For a number of reported facilities, the government was also ordered to supplement the stated basis for finding probable cause to believe that a targeted foreign power was using or about to use the facility. The adequacy of the probable cause statements is not presented by the instant motion.

² For example, (b)(3); (b)(6) [REDACTED] an NSA official, testified at the hearing that NSA maintains (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

I am persuaded that, in all three of these scenarios, NSA could properly initiate surveillance under the above-quoted authority for “later-identified” facilities. For purposes of this provision of the May 31 Order, NSA obtains knowledge of the “nature and location” of a facility when it first assesses that there is probable cause to believe that the facility is being used or about to be used by a targeted foreign power. Thus, “known” in this context applies to both the fact that the target has been found or identified, and a “connecting-the-dots” or understanding of that fact’s significance. A more limited interpretation of this provision would preclude NSA from initiating surveillance under this authority for a facility that, even with the exercise of due diligence, it could not have presented in the original application. I conclude that, under the limited circumstances where this authority applies – only to facilities reasonably believed to be used by non-U.S. persons outside of the United States, on behalf of one of the targeted foreign powers – it is appropriate to grant the government as much latitude in initiating surveillance as the statute can reasonably be construed to permit.

²(...continued)
databases [REDACTED]

³ At the hearing, (b)(3); (b)(6) testified that, since February 2007, NSA had tasked approximately [REDACTED] e-mail addresses and phone numbers for non-FISA collection under Executive Order No. 12333 because they were associated with one of the targeted foreign powers – [REDACTED] than the total number of facilities targeted for surveillance under the probable cause standards of the May 31 Order.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

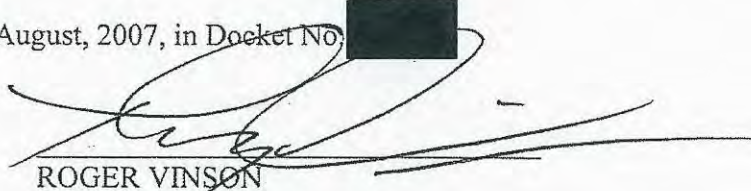
~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

However, I am not able to grant the government the precise relief that its motion requests. The motion proposes that a facility should be eligible for this "later-identified" authority if it had not been the subject of a FISA application or emergency authorization prior to May 24, 2007, or tasked for collection under the authority granted in Docket No. [REDACTED], or under the Terrorist Surveillance Program as of December 31, 2006. Motion at 4-5. These criteria, by their terms, would not preclude the strategic withholding from pre-surveillance judicial review of facilities that were already intended to be subjected to the FISA surveillance at the time the application was submitted. There is no reason to believe that the government has engaged, or would engage, in this practice. However, I conclude that the statute does not permit such an unlimited grant of authority that would, by its terms, allow the initiation of surveillance in those circumstances. The motion is GRANTED only to the extent set out herein.

Accordingly, it is hereby ORDERED that, for purposes of the authority granted pursuant to 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3) on pages 11 and 12 of the May 31 Order, NSA shall be deemed to obtain knowledge of the nature and location of a facility when NSA first is able to determine that there is probable cause to believe that the facility is being used or about to be used by a targeted foreign power. Such determination may be made on the basis, in whole or in part, of analysis of information acquired by NSA on or before May 24, 2007, so long as the analysis that first results in such probable cause assessment was completed after May 24, 2007.

In his order in this docket entered on July 27, 2007, Judge Nathaniel M. Gorton noted the pendency of this motion as a reason for not requiring supplementation of the report filed by the government on July 18, 2007, regarding compliance with this requirement. Accordingly, it is hereby ORDERED that, by August 10, 2007, the government shall supplement that report by providing a statement whether, for each of the reported facilities, NSA was first able to determine that there was probable cause to believe that the facility was being used or about to be used by a targeted foreign power based on an analytical assessment NSA completed subsequent to May 24, 2007. In my view, an affirmative statement in this form should generally suffice to show that this requirement was satisfied. Similar supplementation may be sufficient with respect to the reports required by Judges Kazen, Bates, Benson, Scullin, and Kollar-Kotelly, see footnote 1 above, but I do not decide those issues now.

Done and ordered this 2nd day of August, 2007, in Docket No. [REDACTED]



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~