All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

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

2006 DEC 13 AM 11:04

[redacted]
CLERK

IN RE [redacted]

[redacted] (S)

Docket Number:

[redacted]

EXHIBIT A

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

~~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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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] 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] 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]

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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 powers[3] 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] 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."

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

- 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 o[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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

BACKGROUND

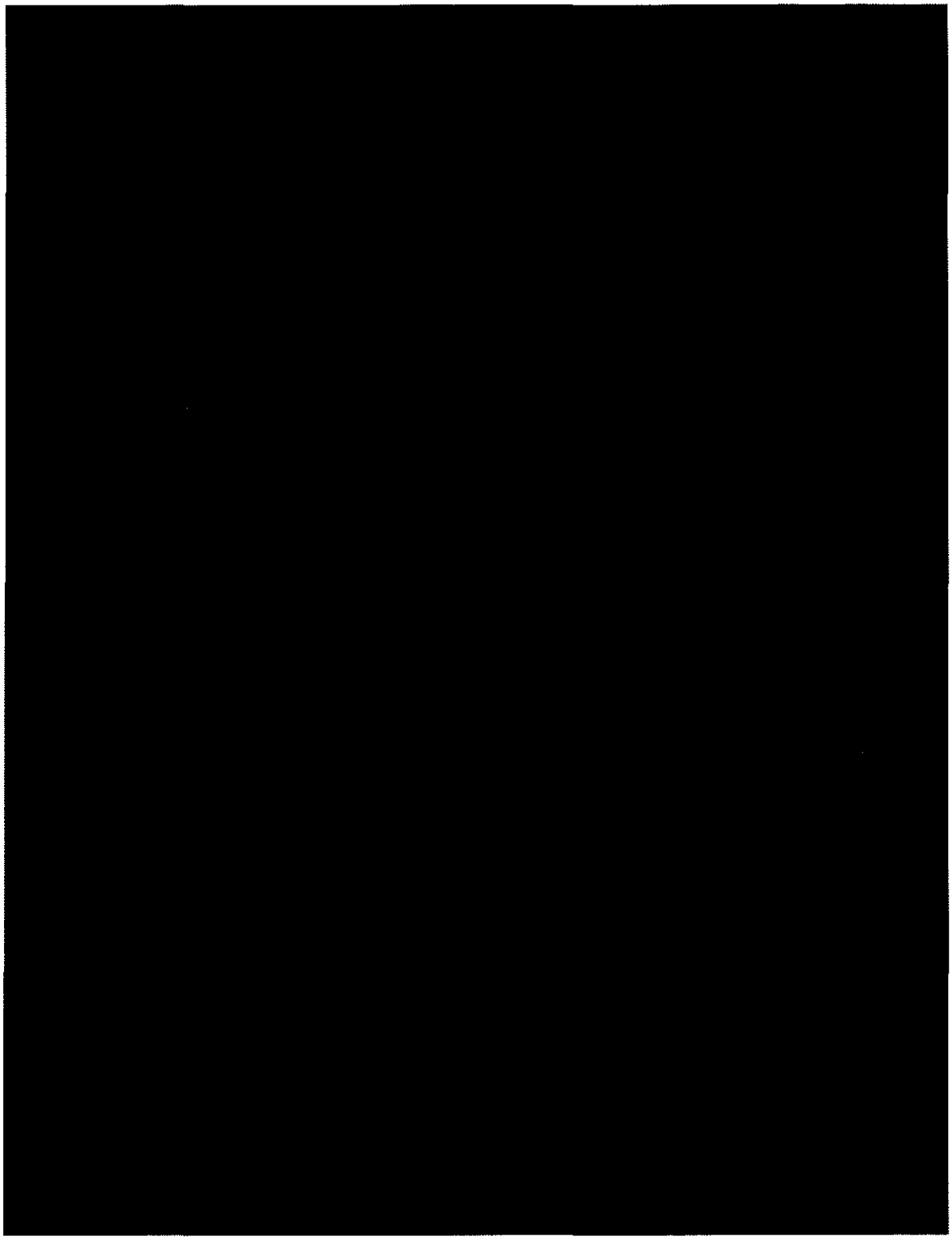
On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners 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.

[redacted]

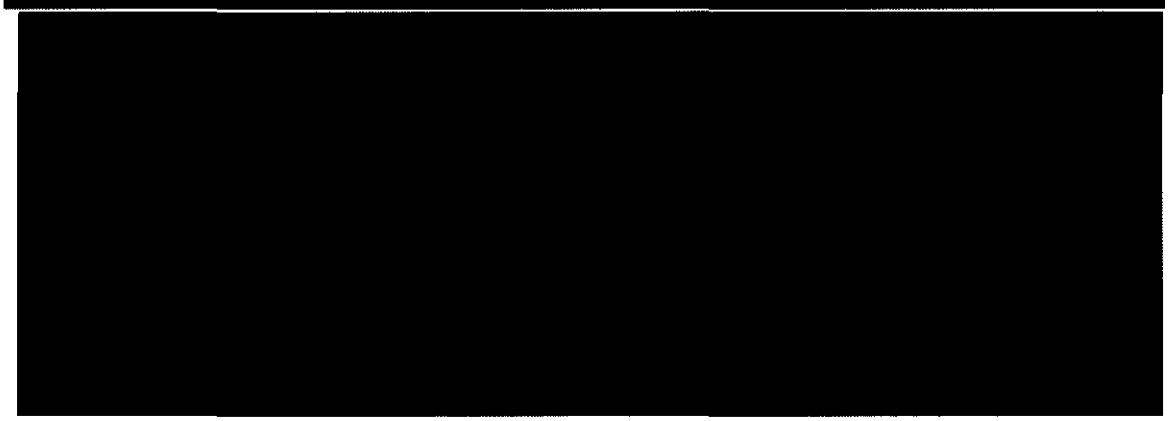
[5] By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

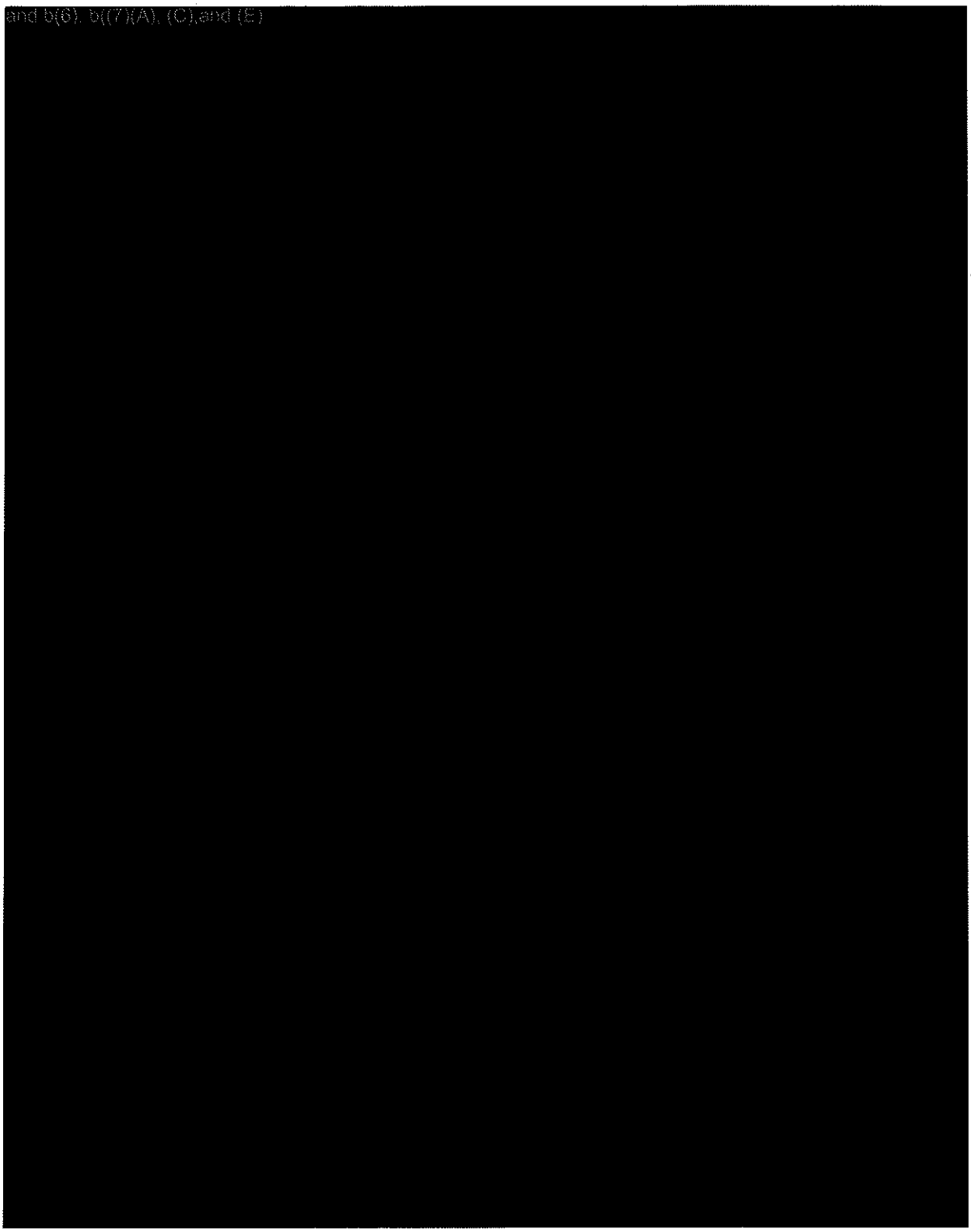
APPROVED FOR PUBLIC RELEASE



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



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



All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[redacted]

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

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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] *See* NCTC Declaration ¶ 152. Similarly, if the Government obtains information suggesting there is probable cause to believe that a particular

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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;

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

(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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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]

[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.

[redacted]

and b(7)(E)

[redacted]

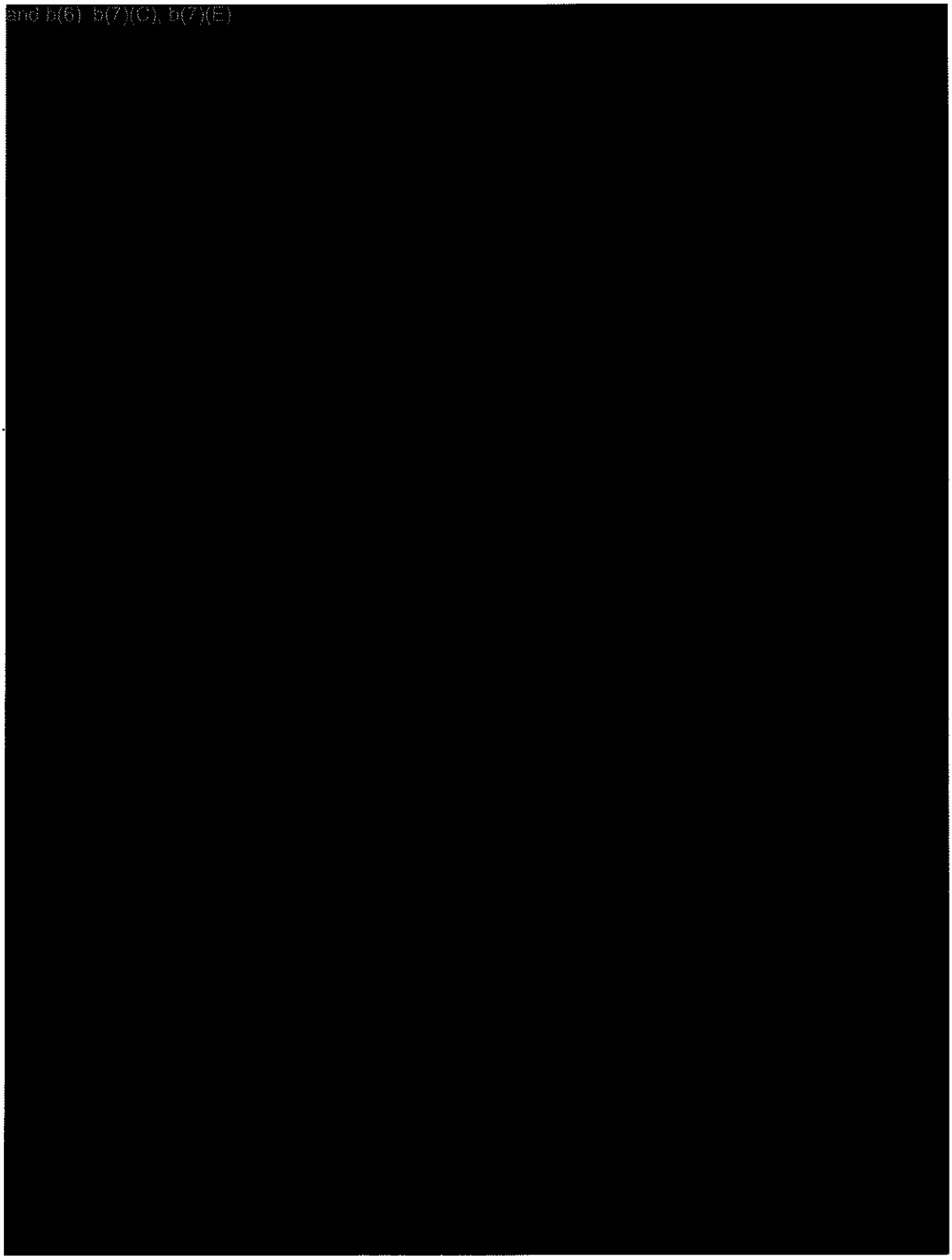
and b(7)(A) and (E)

[redacted]

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

[redacted]

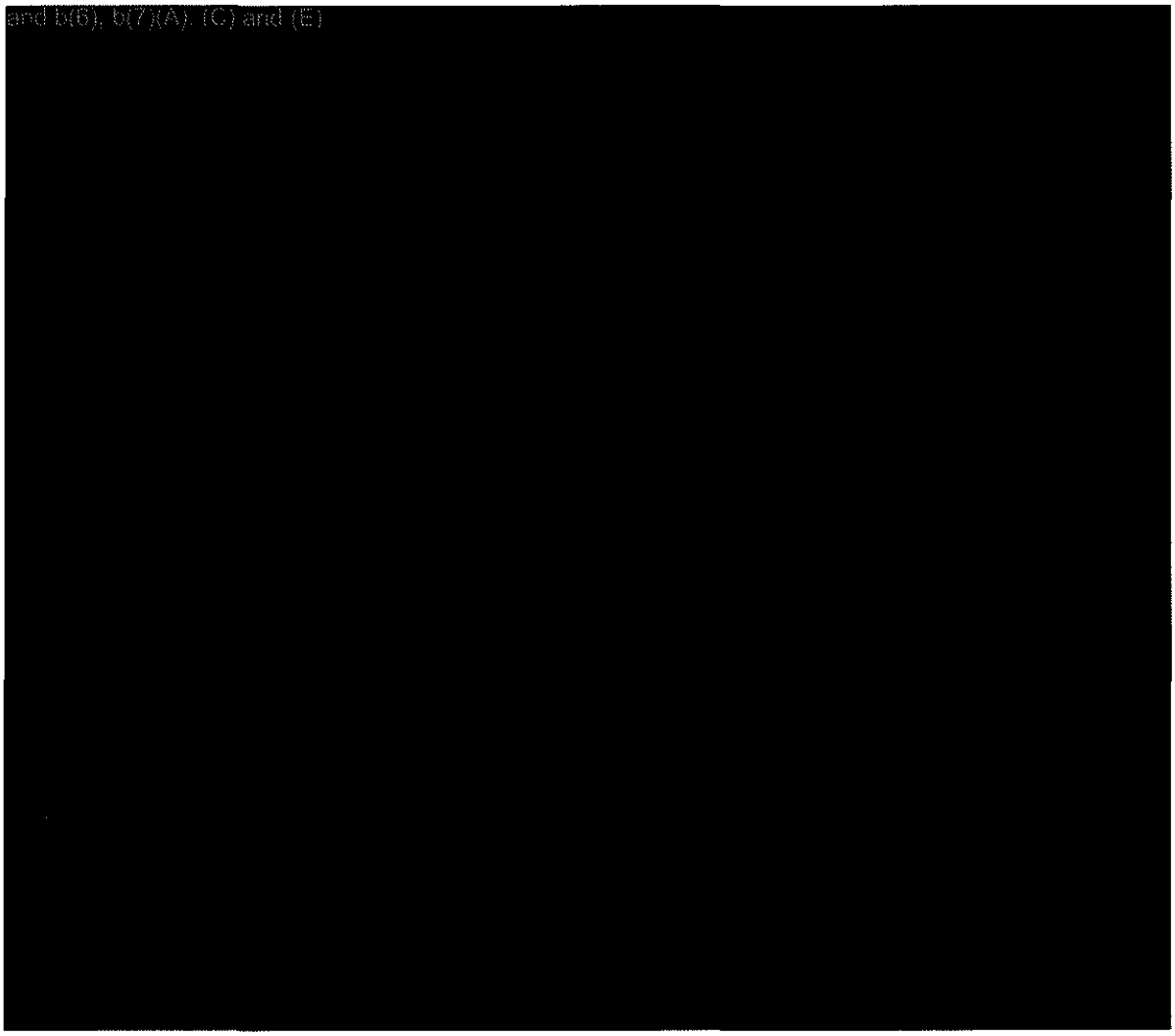
8 [redacted]


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

[redacted]

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE



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

[redacted]

[10]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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* V *The Oxford English Dictionary* 649 (2d ed. 1989)

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

(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]

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

[redacted]

[14] [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]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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]

[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).

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

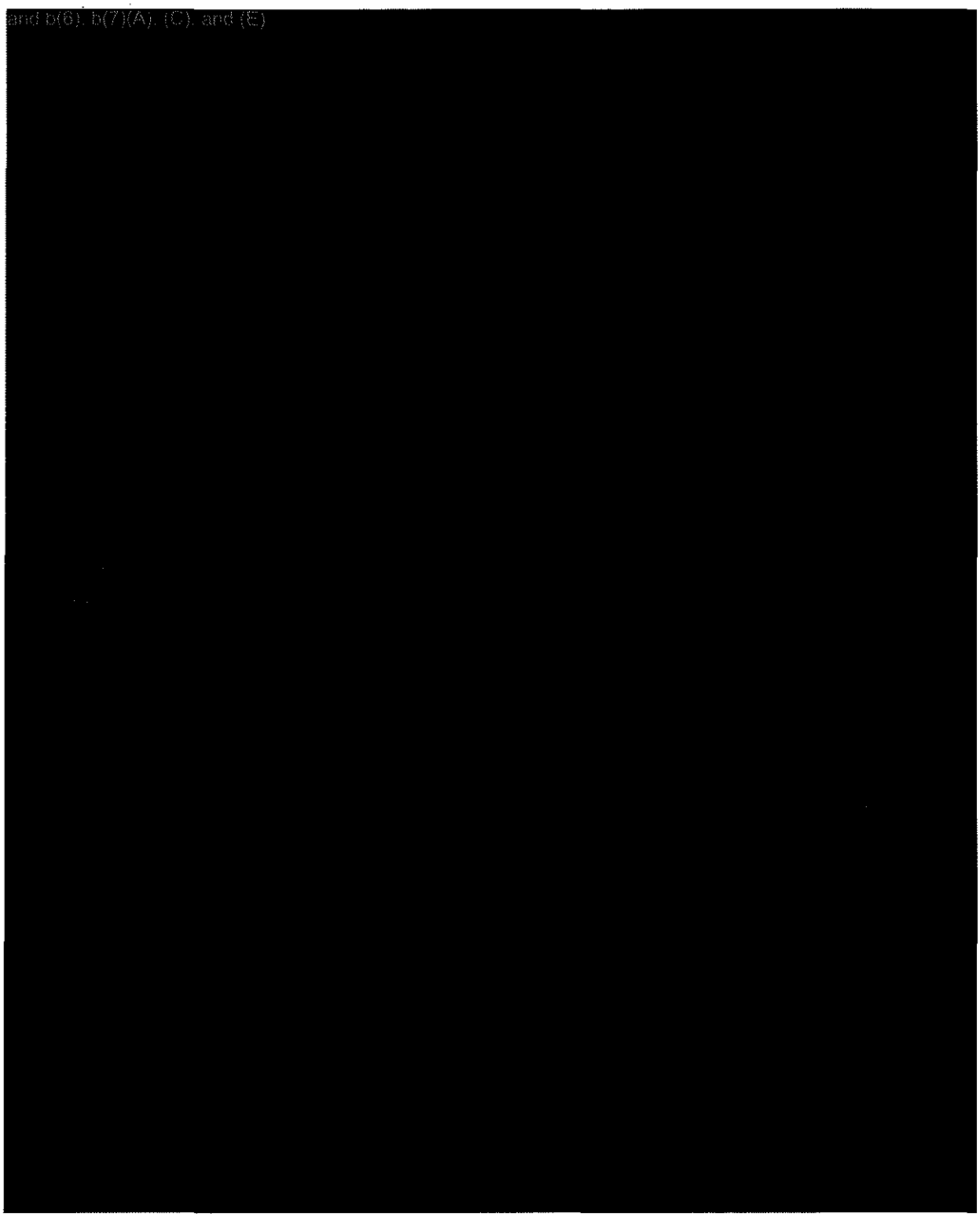
[redacted]

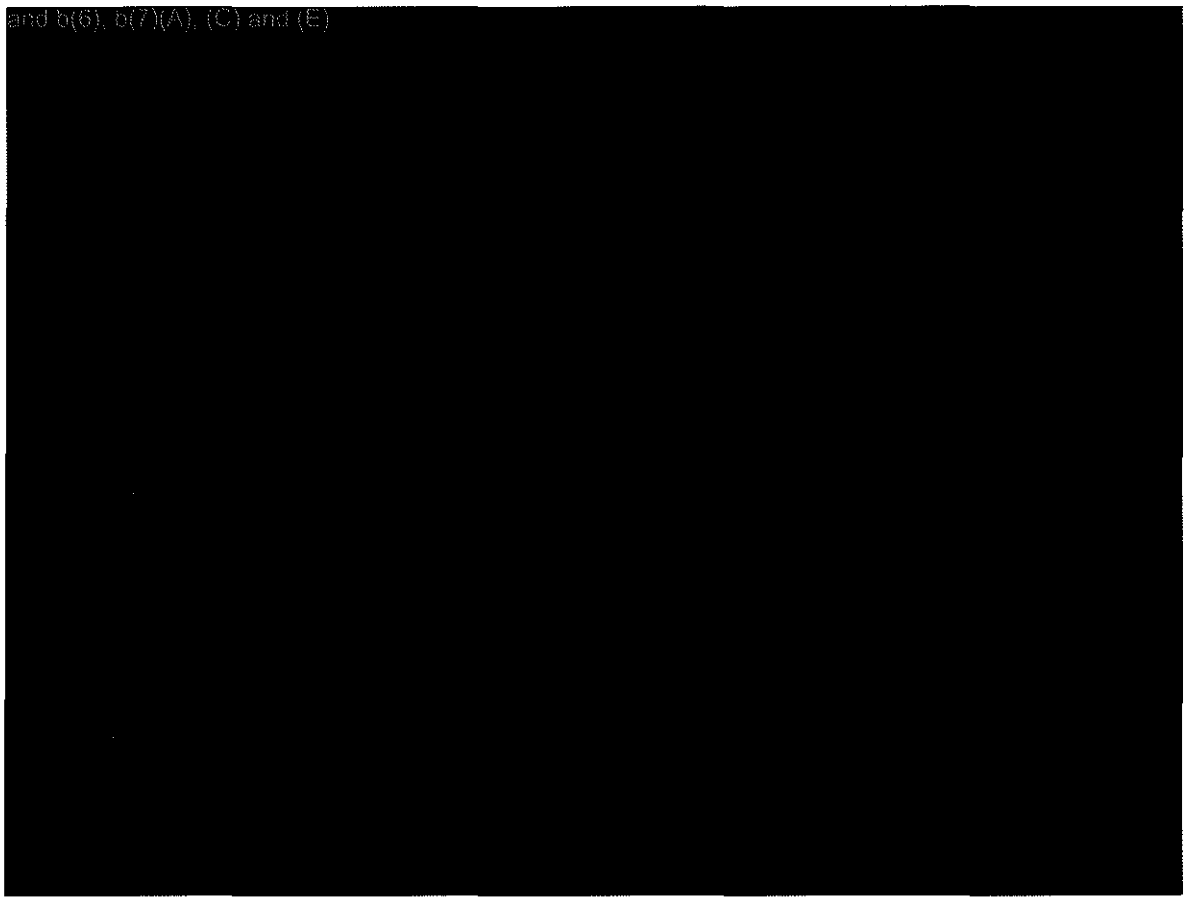
We recognize that this Court has cautioned that the authorization of bulk collection of meta data from electronic communications should not be relied on as a precedent for similar collection of the substantive contents of communications under title I of FISA. *See* [redacted] Order at 49, n.34. The electronic 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] 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]

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE




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

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

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

[redacted]

and b(7)(E)

[redacted]

and b(7)(E)

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

[redacted]

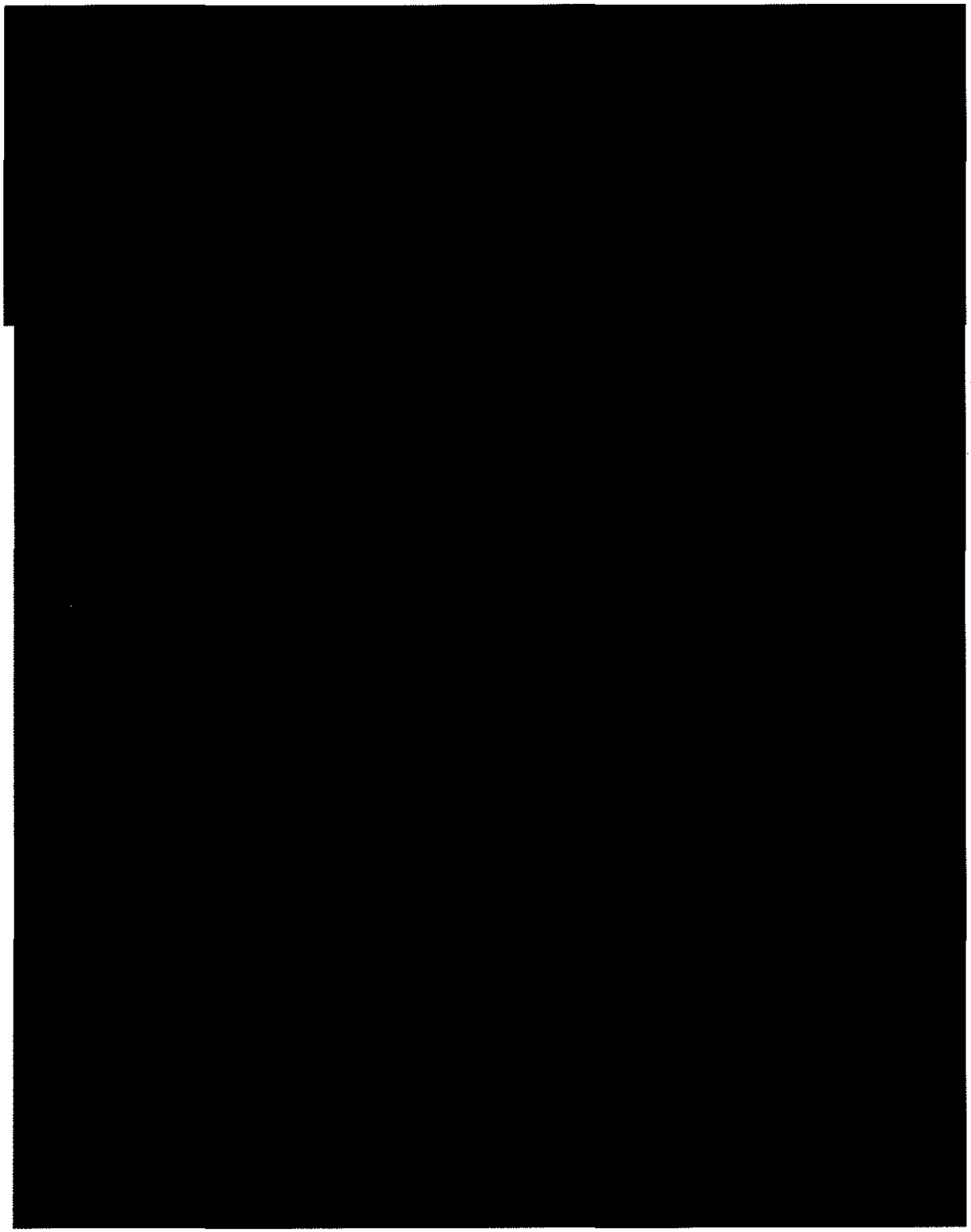
Under section 105(a)(3)(B) of FISA, the Court's order must find that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). As relevant here, FISA defines "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]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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



[redacted]

a vast proportion of the world's Internet traffic is carried at some point on the communications infrastructure in the United States. [redacted]

[redacted]

b(1), b(7)(E) [redacted]

[redacted]

traffic. NSA Declaration ¶ 7. [redacted]

[redacted]

C. **The Minimization Procedures**

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[redacted] We emphasize, however, that the Government has no interest in obtaining all communications [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 believe[19] that: (1) one of the parties to the communication is a member or agent of [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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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]

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

[redacted]

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

[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

[redacted]

[redacted]

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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]

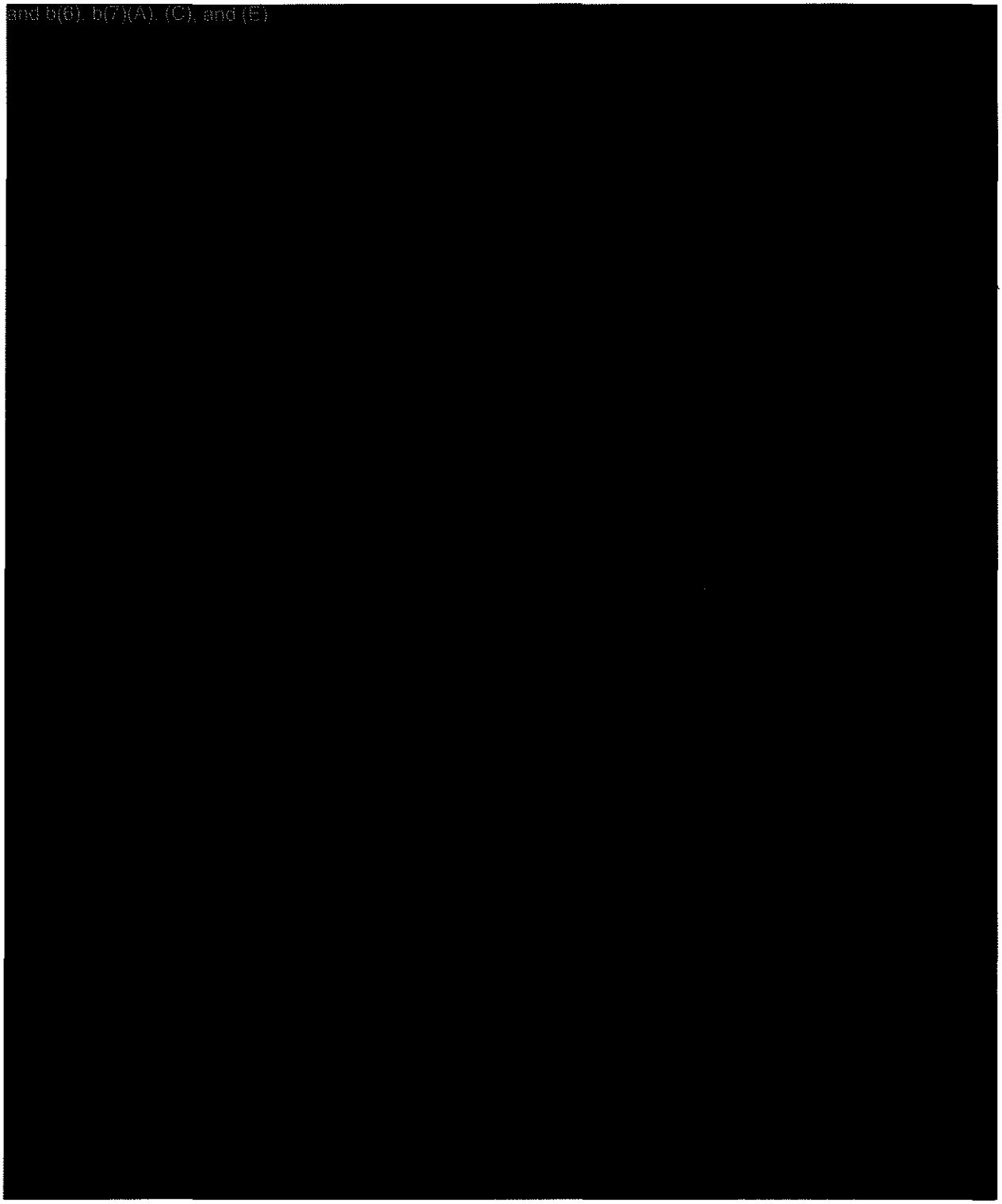
One of the preconditions to the Court's approving an application for electronic surveillance is that the proposed minimization procedures meet the definition of minimization procedures under section 101(h) of FISA. *See* 50 U.S.C. § 1805(a)(4). The Application meets that criterion. According to the portion 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

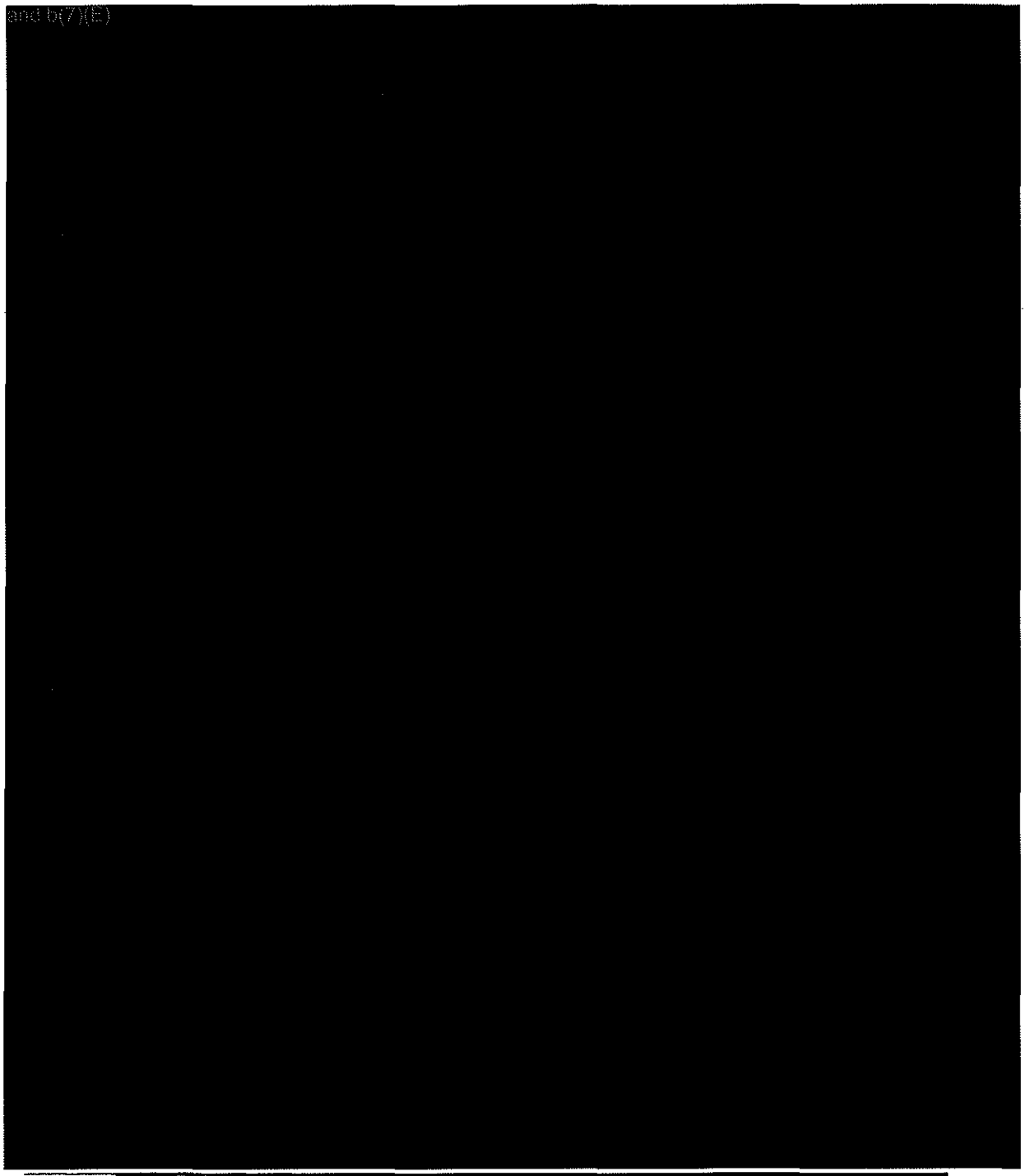
[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

(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)


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



27 and b(7)(E)

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

[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.

[redacted]

[redacted]

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

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

[redacted]

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

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

[redacted]

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

[redacted]

In addition to the particularized minimization procedures designed to acquire only the international communications of individuals who are members or agents of [redacted], 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).

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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]

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. [redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

- 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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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]

[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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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:

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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,

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] *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*,

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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*

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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 (2nd 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] "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] 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] 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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

(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*

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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.

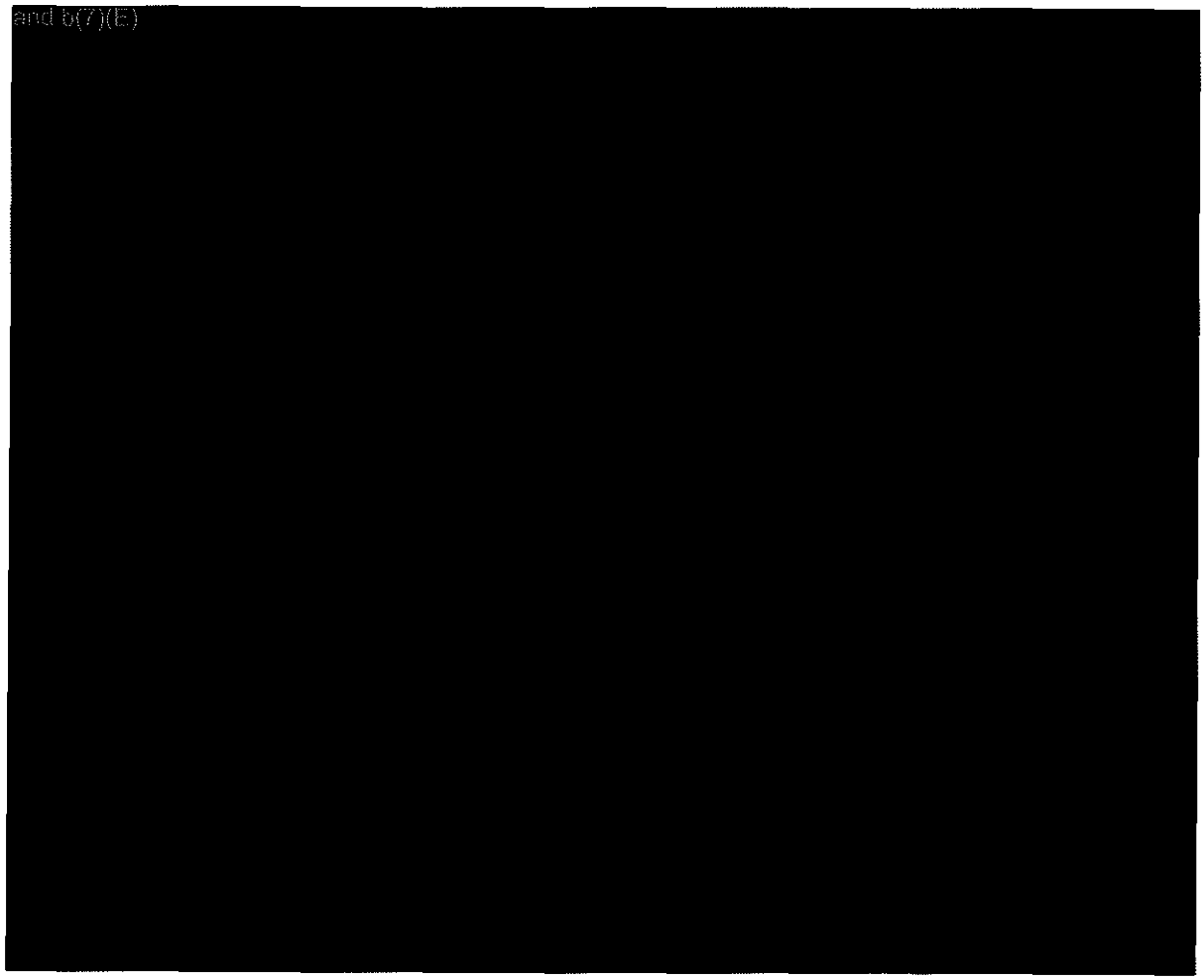
On the other side of the scale here, the Government's interest in conducting the surveillance is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack has already taken thousands of lives and placed the Nation in a state of armed conflict. 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE



We recognize that, because the magnitude of the Government's interest here depends in part upon the threat posed by [redacted] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

believe that any of the new numbers or addresses is associated with a member or agent of [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] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

with a member or agent of [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]

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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

[redacted]
Senior Counsel,
Office of Legal Counsel

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