U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 24, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This responds to your letters, dated February 8 and February 24, 2006, posing questions to Attorney General Gonzales regarding the Terrorist Surveillance Program. The enclosed documents are responsive to all Majority and Minority questions your Committee submitted to the Department of Justice.

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable John Conyers
Ranking Minority Member

RESPONSES TO QUESTIONS FROM CHAIRMAN SENSENBRENNER

1. The Foreign Intelligence Surveillance Court of Review, as the Congressional Research Service (CRS) concedes in its 2006 examination of the NSA program, "is a court of appeals and is the highest court with express authority over [the Foreign Intelligence Surveillance Act,] FISA to address the issue, its reference to inherent constitutional authority for the President to conduct warrantless foreign intelligence surveillance might be interpreted to carry considerable weight."[6] The FISA Court of Review issued an opinion in 2002 that stated "all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority . . . ."[7] The CRS memorandum dated January 5, 2006 does not dispute the fact that all other courts support the proposition that the President has inherent authority to conduct warrantless searches. Instead, the CRS memorandum appears to attempt to downplay these precedents with a statement that the FISA Court of Review's "allusion to the holdings of 'all the other courts to have considered the issue,' appears to have been the cases which pre-date FISA's passage or which address pre-FISA surveillances."[8]

a. Have any courts addressed this issue since the enactment of FISA?
b. Have any courts since the enactment of FISA concluded that the President did not have inherent authority?
c. Does reliance on pre-FISA cases by the FISA Court of Review "[undercut] the persuasive force"[9] of the conclusion that the President has inherent constitutional authority to conduct warrantless surveillance?

As your question states, the FISA Court of Review discussed the President's inherent authority to conduct warrantless electronic surveillance in 2002, twenty-four years *after* FISA was enacted. *See In re Sealed Case*, 310 F.3d 717 (For. Int. Surv. Ct. Rev. 2002). In *Sealed Case*, the Court of Review considered whether the FISA Court had statutory or constitutional authority to place restrictions on the interaction of criminal prosecutors and foreign intelligence investigators as a condition for granting surveillance orders. The Court of Review held that the FISA Court erred by placing those restrictions on the Government. Because prior court decisions had suggested that this was a restriction on the President's constitutional authority, the Court of Review discussed the

---

[6] Elizabeth B. Bazan and Jennifer K. Elsea, 30 Congressional Research Service Memorandum: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, Jan. 5, 2006 [hereinafter CRS Memo].

[7] *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. of Review 2002).

[8] 31 CRS Memo.

[9] 32 CRS Memo.

scope of the President's inherent constitutional authority over foreign intelligence surveillance and whether that authority could be restricted or enhanced by statute. In so doing, the Court of Review recognized that the U.S. Court of Appeals for the Fourth Circuit, "as did all the other courts to have decided the issue, held that the President did have authority to conduct warrantless searches to obtain foreign intelligence information." CRS's suggestion that the Court of Review somehow overlooked that it was relying on pre-FISA cases, thereby undermining its analysis, is entirely without merit. Indeed, the Court of Review was acutely conscious that the decisions it was discussing involved pre-FISA surveillance, and the court noted that fact repeatedly, see 310 F.3d at 725, 726, 742. But that fact does not undercut the decision: the whole point of the opinion was whether and to what extent FISA could modify the standards governing the President's inherent constitutional authority. On this point, the Court of Review was clear: it "took for granted" that the President had inherent constitutional authority to conduct foreign intelligence surveillance and "assuming that is so, FISA could not *encroach* on the President's constitutional power." *Id.* at 742 (emphasis added). In other words, according to the Court of Review, although FISA could supplement the President's power to conduct foreign intelligence surveillance, it could not take away that power, which is vested in him by Article II of the Constitution.

Moreover, as your question correctly observes, no court since the passage of FISA has held to the contrary. For these reasons, the President was entitled to rely on the definitive pronouncement of the specialized court that Congress created to address precisely these matters.

2. In holding that the President has inherent authority to conduct warrantless surveillance, did any of the cases conclude this inherent authority did not arise from the Constitution?

Each of the cases cited in the paper of January 19, 2006 expressly grounded the President's authority to conduct warrantless surveillance in the Constitution. *See United States v. United States District Court ("Keith")*, 407 U.S. 297, 308 (1972) (when discussing the "constitutional powers of the President," reserving any "judgment on the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country"); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-14 (4th Cir. 1980) (stating that the President's authority to conduct warrantless foreign intelligence surveillance arises from the fact that, "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*. The President and his deputies are charged by the constitution with the conduct of the foreign policy of the United States") (emphasis added); *United States v. Butenko*, 494 F.2d 593, 601 (3d Cir. 1974) (*en banc*) (explaining that electronic surveillance is a necessary aid to the President's fulfilling his constitutional responsibilities as "Commander-in-Chief of the Armed Forces and to administer the nation's foreign affairs" and stating that congressional attempts to limit foreign electronic surveillance that "hamper the President's effective performance of his duties in the foreign affairs field would raise constitutional questions"); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973)

("because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence").

3. Is there legal authority to support the proposition drawn from the FISA Court of Review's decision in *In re Sealed Case*,[10] that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework?

The NSA intelligence surveillance activities confirmed by the President involve targeting for interception by the NSA of communications where one party is outside the United States and there is probable cause ("reasonable grounds") to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program" or the "Program"). As set forth below, the Terrorist Surveillance Program is consistent with FISA, and we need not consider whether the President may "gather foreign intelligence outside the FISA framework" to conclude that the Program is lawful.

The Supreme Court has explained that the Authorization for the Use of Military Force of September 18, 2001 (hereinafter "Force Resolution") must be understood to have authorized "fundamental and accepted" incidents of waging war. *Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004) (plurality opinion); *see id.* at 587 (Thomas, J., dissenting). Consistent with this traditional understanding, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force authorization resolutions to permit warrantless surveillance to intercept suspected enemy communications. *Cf.* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, "Congress intended to authorize the President to take at least those actions permitted by the laws of war"). The Force Resolution thus authorizes the President to conduct the Terrorist Surveillance Program against al Qaeda and affiliated terrorist organizations. FISA itself contemplates that a later enactment, such as the Force Resolution, could authorize electronic surveillance because it provides that electronic surveillance is not prohibited if it is "authorized by statute." 50 U.S.C. § 1809(a).

In addition, substantial authority indicates that the President has inherent constitutional authority over the gathering of foreign intelligence—authority that Congress may not circumscribe. The Foreign Intelligence Surveillance Court of Review suggested that, even after FISA, the President possesses inherent constitutional authority that FISA could not limit. *In re Sealed Case*, 310 F.3d 717, 742 (2002). As the court stated: "all the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power."

[10] *See* 310 F.3d at 746.

Id. This specialized court that Congress created for the very purpose of hearing appeals from the FISA court is not the only court to suggest that the President maintains some constitutional authority to conduct foreign intelligence surveillance that may not be limited by Congress. The Third Circuit explained that the gathering of foreign intelligence is essential to fulfilling the President's constitutional responsibilities as "Commander-in-Chief of the Armed Forces and to administer the nation's foreign affairs." *United States v. Butenko*, 494 F.2d 593, 601 (1974) (*en banc*). Congressionally imposed limitations on that power may so "hamper . . . the President's effective performance of his duties in the foreign affairs field [to] raise[] constitutional questions." *Id.* For that reason, the court interpreted a statute that preceded FISA as not limiting the President's constitutional authority to conduct foreign intelligence surveillance. *Id*. These considerations are particularly pressing in the context in which the Terrorist Surveillance Program operates; for, in a time of congressionally authorized armed conflict, the President's constitutional power is at its apex.

4. In *In re Sealed Case* the Court of Review states, in part, "Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance…."[11] The January 5, 2006 CRS memorandum asserts that one approach to interpreting this and other Court of Review statements would be to interpret them "as referring to the President's inherent authority to conduct such surveillances outside the scope of 'electronic surveillance' under FISA. In essence, the court's statements would then be seen as a reference to presidential authority over those areas of NSA activities which were intentionally excluded from FISA when it was enacted. Alternatively, it might be argued that the court's statements may refer to continuing exercise of inherent presidential authority within the FISA structure, which the Court of Review found to be constitutional."[12] Does the President adhere to either of these approaches to support the program?

The Terrorist Surveillance Program does not rely on either of those rationales. As described above, the Foreign Intelligence Court of Review analyzed whether and to what extent Congress could augment the President's inherent constitutional authority to conduct foreign intelligence surveillance. By stating that "FISA could not encroach on the President's constitutional power," the Court of Review made clear its opinion that there are certain foreign intelligence surveillance matters for which Congress cannot limit the President's authority. Although the Court of Review did not describe the precise contours of the President's constitutional authority to conduct foreign intelligence surveillance, *see In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002), the President's authority is at its zenith with respect to the circumstances of the Terrorist Surveillance Program. The President has ordered foreign intelligence surveillance of the declared enemy of the United States in a time of a congressionally authorized armed

[11] *Id.*

[12] 32 CRS Memo.

conflict. Because the Force Resolution authorizes the limited Terrorist Surveillance Program, we need not demarcate the limits of the President's constitutional authority.

5. Some have questioned whether President Carter's signature on FISA in 1978, together with his signing statement, was an explicit renunciation of any claim to inherent Executive authority under Article II of the Constitution to conduct warrantless surveillance.

a. Does Congress have the authority to renounce any inherent presidential authority?

b. Is there any case law that supports or proscribes Congress' ability to renounce inherent presidential authority?

The Constitution is the supreme law of the land, and any statutes inconsistent with the Constitution must yield. This basic principle of our system of government means that no President, merely by assenting to a piece of legislation, can diminish the scope of the President's constitutional power. *See New York v. United States*, 505 U.S. 144, 182 (1992) ("The constitutional authority of Congress cannot be expanded by the 'consent' of the governmental unit whose domain is thereby narrowed, whether that unit is the Executive Branch or the States.") (collecting authorities). Nor do we believe that President Carter attempted to do so by signing FISA. President Carter's Attorney General testified at a hearing on FISA as follows: "[T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution*. It simply, in my view, is not necessary to state that power, so there is no reason to reiterate or iterate it as the case may be. It is in the Constitution, whatever it is. The President, by offering this legislation, is agreeing to follow the statutory procedure." Hearing Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence (Jan. 10, 1978) (emphasis added).

Just as one President may not, through signing legislation, eliminate the Executive Branch's inherent constitutional powers, Congress may not "renounce inherent presidential authority." The Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g.*, *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and Congress may not "impede the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988); *see also id*. at 696-97. Congress certainly may obviate the need to determine the precise contours of the President's inviolable constitutional authority, *see Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at is maximum, *for it includes all that he possesses in his own right plus all that Congress can delegate*.") (emphasis added). And that is the case here, as Congress authorized the President to undertake the fundamental and accepted incidents of war, including signals intelligence targeted at the enemy, through the Force Resolution

6. Has any other President held that the President has this inherent authority? If so, has any other President used such an authority prior to and after the enactment of FISA?

Presidents long have relied on their inherent constitutional authority to conduct foreign intelligence surveillance. President Wilson, for example, relying only on his constitutional powers and a congressional authorization for use of force, authorized the interception of *all* telephone, telegraph, and cable communications into and out of the United States during World War I. *See* Exec. Order 2604 (Apr. 28, 1917). Similarly, President Roosevelt authorized the interception of "*all . . . telecommunications traffic* in and out of the United States." The Clinton Administration also relied on inherent constitutional authority in authorizing warrantless physical searches to collect foreign intelligence information. Jamie Gorelick, Deputy Attorney General in the Clinton Administration, testified before Congress in 1994, when Congress was considering a since-enacted proposal to amend FISA to permit court authorization of physical searches for foreign intelligence purposes, that the President has inherent authority under the Constitution to conduct foreign intelligence searches in the United States without a warrant, and that such warrantless searches are permissible under the Fourth Amendment. *See* Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence, 103d Cong. 2d Sess. 61, 64 (1994) (statement of Deputy Attorney General Jamie S. Gorelick). *See also In re Sealed Case*, 310 F.3d at 745-46. The history of Presidents' employing signals intelligence pursuant to their constitutional authority is detailed in the Justice Department's paper of January 19, 2006. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 14-18 (Jan. 19, 2006).

7. The Department of Justice has stated that Congress has confirmed and supplemented the President's inherent authority by statute through the Authorization for the Use of Military Force (AUMF).[13] Please explain specifically how the AUMF has "confirmed and supplemented"[14] the President's inherent authority with respect to warrantless surveillance.

The Force Resolution "confirm[s]" the President's inherent authority in this area by expressly recognizing that the September 11th attacks "render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad." Force Resolution pmbl. The Resolution states that the attacks "continue to pose an unusual and extraordinary threat to the national security." *Id*. Finally, Congress explicitly affirmed that "the President has authority under the Constitution to take action to deter and prevent actions of international terrorism against the United States." *Id*.

---

[13] *See* Pub. L. no. 107-40 § 2(a); 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541).

[14] Department of Justice, 2 LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT, Jan 19, 2006.

The Force Resolution "supplement[s]" the President's inherent authority by authorizing the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the terrorist attacks of September 11th in order to prevent "any future acts of international terrorism against the United States." The Force Resolution is framed in broad and powerful terms, and a majority of the Justices of the Supreme Court concluded in *Hamdi v. Rumsfeld* that the Force Resolution authorized the "fundamental and accepted" incidents of the use of military force. *Cf.* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, "Congress intended to authorize the President to take at least those actions permitted by the laws of war"). As set forth at greater length in the Department's January 19th paper, signals intelligence is a fundamental and accepted incident of the use of force during wartime. Moreover, when it enacted the Force Resolution, Congress was legislating in light of the fact that past Presidents (including Woodrow Wilson and Franklin Roosevelt, as noted above) had interpreted similarly broad resolutions to authorize much wider warrantless interception of international communications.

8. On December 19, 2005, *USA Today* reported that the President's executive order that authorized the surveillance program represented a "dramatic shift from restrictions on domestic spying imposed after exposure in the mid-1970s of NSA operations against U.S. citizens."[15]

a. Is this claim substantiated?
b. Have previous Administrations, at the very least, recognized the President's Constitutional duty to authorize similar programs related to national security?
c. The same article asserted that the Communications Act of 1934 as well as the U.S. Criminal Code have provisions that limit or ban the interception of electronic communications. How do these laws effect the President's prerogative to authorize the NSA program?

The Terrorist Surveillance Program is narrowly tailored to target only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof, *see Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"), and "probable cause" is the standard employed under FISA for approving applications for electronic surveillance.

As explained in the Department of Justice's paper of January 19, 2006, the prohibitions on unauthorized surveillance set forth in FISA and chapter 119 of title 18,

[15] John Diamond, *NSA's Surveillance of Citizens Echoes 1970s Controversy; Bush Denies Post-9/11 Order Clashes with 1978 Law Requiring Warrants*, USA Today, Dec. 19, 2005, at A6.

United States Code, must be read in light of section 109(a) of FISA, which explicitly contemplates that statutes can authorize intelligence surveillance outside the procedures set forth in FISA. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 18-21.

Section 605 of the Communications Act of 1934 prohibits "divulg[ing] or publish[ing]" the content or existence of interstate or foreign communications by wire or radio. *See* 47 U.S.C. § 605(a). This has long been viewed as inapplicable to the government's collection of foreign intelligence. President Roosevelt determined that those provisions do not prohibit federal government officials from gathering foreign intelligence for use within the Executive Branch, because the gathering of such information by the government does not constitute "divulg[ing] or publish[ing]" the communication. On the basis of this legal determination, President Roosevelt ordered the interception of "all telecommunications traffic" into or out of the United States. Memorandum from President Roosevelt (May 21, 1940), *reproduced in United States v. United States District Court*, 444 F.2d 651, 670 (6th Cir. 1971) (Appendix A).

9. In a January 6, 2006 letter from Professor Laurence Tribe to Congressman Conyers, the Professor states that the National Security Agency program "in question, far from being *authorized* by Congress, flies in the fact of an *explicit congressional prohibition* and is therefore unconstitutional without regard to the Fourth Amendment… The inevitable conclusion is that the AUMF did not implicitly authorize what the FISA expressly prohibited. It follows that the presidential program of surveillance at issue here is a separation of powers as grave an abuse of executive authority as I can recall ever having studied."[16] Do you agree that FISA "expressly prohibits" the specific activities authorized under this program?

We disagree with Professor Tribe's assertion that the Terrorist Surveillance Program runs into an "express congressional prohibition." Section 109 of FISA itself contemplates that intelligence surveillance can be authorized by statutes other than FISA. 50 U.S.C. § 1809(a). Thus, FISA does not define the universe of permissible intelligence surveillance, and it does not close the door on subsequent congressional authorizations of electronic surveillance. Indeed, it is doubtful that one Congress *could* bind future Congresses in such a way. Instead, FISA reflects the understanding that later-enacted statutes could authorize electronic surveillance as circumstances warrant.

The Force Resolution is precisely such a statute. In the Force Resolution, Congress authorized the President to use "all necessary and appropriate force against those nations, organizations, or persons" that "[the President] determines" to be responsible for the September 11th attacks. In this context, five Justices of the Supreme Court identified the proper mode for analyzing which powers accompany the Force Resolution. They concluded that the Force Resolution satisfied a statute nearly identical to section 109 of FISA, 18 U.S.C. § 4001(a), which prohibits the detention of United States citizens "except pursuant to an Act of Congress." *See Hamdi v. Rumsfeld*, 542

[16] Letter from Laurence Tribe to Representative John Conyers (Jan. 6, 2006), at 2.

U.S. 507, 519 (plurality opinion); *id.* at 587 (Thomas, J., dissenting). Just as it satisfies section 4001, the Force Resolution satisfies FISA's provisions for statutory authorizations for intelligence surveillance. For that reason, it is simply incorrect to suggest that the Terrorist Surveillance Program "flies in the face of an explicit congressional prohibition." In his letter, Professor Tribe did not confront the wholly analogous effect of the Force Resolution on 18 U.S.C. § 4001, prohibiting detention.

10. If FISA were read to prohibit the President from taking steps he deemed necessary to protect the United States during wartime, would the constitutionality of that Act be called into question? Please explain in detail what constitutional problems or questions may arise if it were determined that FISA, separately or in conjunction with the AUMF, prohibits the President from authorizing the terrorist surveillance program.

As explained above, the Force Resolution authorizes the use of signals intelligence against al Qaeda and affiliated terrorist organizations. But even if there were some ambiguity with respect to whether FISA can be read, together with the Force Resolution, to allow the Terrorist Surveillance Program, the President's inherent powers as Commander in Chief and as chief representative of the Nation in foreign affairs to undertake signals intelligence against the declared enemy of the United States during an armed conflict would require resolving such ambiguity in favor of the President's authority. Under the canon of constitutional avoidance, statutes are interpreted to avoid serious constitutional questions where "fairly possible." *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). The canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Thus, there is no need to confront the question whether FISA would be unconstitutional if, contrary to the correct interpretation of the Force Resolution and FISA, the Terrorist Surveillance Program were somehow statutorily prohibited.

The constitutional problems that would be raised by a contrary interpretation of the statute are serious. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation's foreign affairs. As the Supreme Court has explained, "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g., The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g., Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

Based on that constitutional authority, the Department of Justice, in both Democratic and Republican administrations, has recognized the President's inherent authority to authorize foreign intelligence surveillance. President Carter's Attorney General, Griffin Bell, testified at a hearing on FISA as follows: "[T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution*." Hearing Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence (Jan. 10, 1978) (emphasis added). More recently, the Foreign Intelligence Surveillance Court of Review recognized that the President has inherent constitutional authority to gather foreign intelligence that cannot be intruded upon by Congress. The court explained that all courts to have addressed the issue of the President's inherent authority have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case*, 310 F.3d 717, 742 (2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, assuming that is so, "*FISA could not encroach on the President's constitutional power*." *Id.* (emphasis added). It is important to remember that virtually every court that has concluded that the President has inherent authority to conduct foreign intelligence surveillance did so during a time of peace. During an armed conflict, of course, the President's constitutional power is at its apex, making a hypothetical attempt by Congress to interfere with the President's inherent authority all the more constitutionally troubling. Congress may not "impede the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988); *see also id*. at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation.

11. The January 5, 2006 CRS Memorandum quotes a December 22, 2005 letter from the DOJ Office of Legislative Affairs that says, "But under established principles of statutory construction, the AUMF and FISA must be construed in harmony to avoid any potential conflict between FISA and the President's Article II authority as Commander in Chief." The memorandum, however, concludes, on this point, that "It is unclear how FISA and the AUMF are seen to collide. Principles of statutory construction generally provide guidance for interpreting Congress's intent with respect to a statute where the text is ambiguous or a plain reading leads to anomalous results; and where possible, a statute that might be read in such a way as to violate the Constitution is to be construed to avoid the violation. However, such principles are only to be applied where there is a genuine ambiguity or conflict between two statutes, and where there is some possible reading that might avoid a conflict…."[17] A contrary view has been presented by constitutional scholar Robert Alt, that "if from some reason a court finds that there is a conflict between the AUMF and FISA, then standard rules of statutory interpretation suggest that the AUMF must control. Specifically, the AUMF contains a savings clause, making clear that the statute does not

[17] 41 CRS Memo.

intend to impair the operation of the War Powers Resolution. *See* AUMF, § 2(b)(2) (Nothing in this resolution supercedes any requirement of the War Powers Resolution.). The canon of *expressio unius est exclusio alterius* requires that Congress, having created an express exception for a statute intended to limit Presidential power, must have excepted FISA if they intended to exempt it from any conflict with the AUMF. They did not, and so the AUMF must control if the statutes are seen as conflicting."[18] (*See* enclosure)

a. Which analysis is correct? Please explain why you agree or disagree with these analyses.
b. Do FISA, the AUMF, and the NSA program conflict?

It is not the position of the Justice Department that FISA and the Force Resolution "collide." Indeed, the Force Resolution and FISA are perfectly consistent with each other. By expressly providing that other statutes may authorize electronic surveillance, FISA contemplates that statutes such as the Force Resolution could authorize electronic surveillance—outside the procedures of FISA. In this respect, the Force Resolution is precisely the type of limited, context-specific authorization that FISA anticipates during periods of armed conflict. Thus, interpreting the Force Resolution and FISA to permit the Terrorist Surveillance Program is not only "some possible reading," it is the *correct* reading.

The Force Resolution authorizes the use of intelligence surveillance as an incident of force directed against al Qaeda and affiliated terrorist organizations, and FISA permits such future authorizations by Congress as circumstances warrant. The canon of constitutional avoidance comes into play only to the extent that the proper interpretation of these statutes is not otherwise clear. It suggests that, insofar as there is any ambiguity whether FISA, read in light of the Force Resolution, authorizes the Terrorist Surveillance Program, that ambiguity must be resolved to allow the President to authorize the Terrorist Surveillance Program—an early warning system critical to the defense of the Nation. Here, however, we do not believe that there is a "genuine ambiguity," because the authorization of the Program by these two statutes is clear.

Finally, we believe that Professor Alt's reasoning provides yet another reason to interpret the Force Resolution and FISA together to authorize the Terrorist Surveillance Program. To the extent that some have argued that FISA stands as a virtually immovable barrier that must be repealed or specifically amended, Professor Alt's analysis goes some way to establishing that such is indeed the effect of the Force Resolution. The Force Resolution expressly preserves a statute that purports to limit the President's discretion in a time of war. Under the *expressio unius* canon, the Force Resolution's explicit preservation of the War Powers Resolution suggests that other statutes that would limit the President's use of "necessary and appropriate force" would yield to the Force Resolution. In this way, to the extent that FISA actually limits the President's ability to employ signals intelligence—a fundamental incident of the use of force—against the

[18] Letter from Robert Alt to Chairman Sensenbrenner (Feb. 3, 2006), at 8.

declared enemy of the United States, the Force Resolution would vitiate those restrictions. That reading is consistent with the decision in *Hamdi*, where a majority of the Justices concluded that the Force Resolution satisfied a statutory restriction on detention (18 U.S.C. § 4001) that was nowhere mentioned in the Force Resolution. Professor Alt's reasoning provides still more justification for concluding that the Force Resolution would, if necessary, repeal FISA to the extent it prevents the President from making use of the fundamental and accepted incidents of the use of military force in the armed conflict against al Qaeda.

12. Please explain how the NSA terrorist surveillance program relates to FISA. In doing so, please explain how the program — which operates outside the context of FISA — is consistent with FISA, given that FISA — provides it shall be the "exclusive means by which electronic surveillance, as defined in section 101 of [FISA], and the interception of domestic wire, oral, and electronic communications may be conducted."[19]

Before answering this question, we note that the Department's legal analysis assumes, solely for purposes of that analysis, that the targeted interception of international communications authorized under the Terrorist Surveillance Program would constitute "electronic surveillance" as defined by FISA. As noted in our January 19th paper, we cannot confirm whether that is actually the case without disclosing sensitive classified information.

Section 2511(2)(f) of title 18 states that the "procedures in [chapter 119 of title 18] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted." But this provision must be read together with FISA, including section 109(a). Section 109(a) expressly contemplates that another "statute" can authorize electronic surveillance and thereby expressly incorporates such future enactments into the FISA framework. Section 109(a) is a means within FISA, and thus reliance on the Force Resolution satisfies section 2511(2)(f)'s admonition that FISA is the "exclusive means" for conducting certain forms of electronic surveillance. Reading FISA to permit electronic surveillance authorized by another statute makes particular sense because, as detailed at pages 22 and 23 of the Department's January 19th paper, at the time of FISA's enactment, provisions of law besides FISA and chapter 119 of title 18 authorized the interception of "electronic surveillance" and there is no indication that FISA purported to outlaw that practice. For example, in 1978, use of a pen register or trap and trace device constituted "electronic surveillance" under FISA. While FISA authorized use of pen registers, chapter 119 of title 18 did not. Thus, if FISA did not contemplate electronic surveillance authorized under another statute, the use of pen registers other than to collect foreign intelligence would have been illegal. That cannot have been the case, and no court has held that pen registers could not be authorized outside the foreign intelligence context.

[19] 18 U.S.C. § 2511(2)(f).

This reading of section 2511(2)(f) is also supported by its legislative history, which indicates an intent to prevent the President from engaging in surveillance except as authorized by Congress. Although section 2511(2)(f) mentions only FISA and chapter 119 of title 18, the House Conference Report explains that section 2511(2)(f) set forth all then-existing statutory restrictions on electronic surveillance and cautioned the President not to engage in such surveillance outside of congressionally sanctioned parameters. *See* H.R. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. It was not directed at restricting the manner in which Congress could subsequently authorize electronic surveillance.

13. Some are concerned that NSA's use of this authority erodes the Department of Justice's authority to conduct wiretaps under FISA. Do you agree with this concern?

FISA remains an essential and invaluable tool for foreign intelligence collection, both in the armed conflict with al Qaeda and in other contexts. In contrast to surveillance conducted pursuant to the Force Resolution, FISA is not limited to the conflict against al Qaeda and affiliated terrorist organizations. In addition, FISA has procedures that facilitate the use of evidence in criminal prosecutions while, at the same time, protecting intelligence sources and methods. In this instance, the Force Resolution provides the President with another means for conducting intelligence surveillance against al Qaeda and related terrorist organizations.

14. Does the fact that Congress amended FISA in response to the terrorists attacks on September 11, 2001, "[bolster] the notion that FISA is intended to remain fully applicable," as asserted by the January 5, 2006 CRS Memorandum?[20]

The amendments to FISA after the September 11th attacks are fully consistent with the Department's explanation of the legal authorities supporting the Terrorist Surveillance Program. It is important to emphasize that the Terrorist Surveillance Program is limited to communications where one party is outside the United States and there is probable cause ("reasonable grounds") to believe that at least one party is a member of al Qaeda or an affiliated terrorist organization—the organizations that the President determined were responsible for the September 11th attacks. But foreign intelligence surveillance is also necessary to detect and prevent potential attacks from other, unrelated terrorist groups, as well as for a variety of purposes that have nothing to do with terrorism. These amendments to FISA enacted after September 11th were crucial to correct certain systemic problems in the FISA process that impaired its effective functioning across the board, not simply with respect to the armed conflict against al Qaeda.

Of particular importance were modifications that removed the "wall" between intelligence officers and criminal law enforcement officers. *See In re Sealed Case*, 310

[20] 37 CRS Memo.

F.3d 717, 725-30 (Foreign. Int. Surv. Ct. Rev. 2002). This "wall" was identified as crippling the Government's use of foreign intelligence information well before the September 11th attacks and in contexts unrelated to terrorism. *See, e.g.*, *Final Report of the Attorney General's Review Team on the Handling of Las Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); GAO, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Matters is Limited* (GAO-01-780) 3, 31 (July 2001); *see also The 9/11 Commission Report* 78-81, 424 (2004). Although the existence of the "wall" undermined the fight against al Qaeda, it also impaired the Government's ability to conduct foreign intelligence surveillance in other critical contexts. Thus, the amendments to FISA made after the September 11th attacks in no way undermine the conclusion that Congress authorized electronic surveillance for the particular conflict against al Qaeda through separate legislation.

15. What is the rationale for authorizing a program to conduct surveillance in a manner that does not require prior judicial review by the FISA Court?

After September 11th, speed and agility were especially crucial in fulfilling the President's constitutional obligation of protecting the Nation from further attacks. The Terrorist Surveillance Program targets communications only where one party is outside the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. FISA itself uses a "probable cause" standard. Among the advantages offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination and how many layers of review must occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communication systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. Relying on the best available intelligence, these officers determine before intercepting any communications whether there is probable cause to believe that one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

By contrast, pursuing "prior judicial review by the FISA court" requires significantly more time. In order to obtain judicial review by the FISA court before conducting surveillance, the Government must assemble a voluminous application, obtain the approval of the Attorney General himself and senior administration national security officials, submit the materials to the court, and await its decision. Also, because FISA requires the Attorney General to "reasonably determine[]" that "the factual basis for issuance of" a FISA order exists at the time he approves an emergency authorization, *see* 50 U.S.C. § 1805(f)(2), as a practical matter, it is necessary for NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General to review a matter before even emergency surveillance would begin. Great care must be exercised in reviewing requests for emergency surveillance because of the risks involved. Among other things, if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, there is a risk that the court would disclose the surveillance to U.S. persons whose communications were intercepted, *see* 50 U.S.C.

§ 1806(j), potentially compromising ongoing intelligence efforts. The Terrorist Surveillance Program allows experienced intelligence officials to begin surveillance quickly while still safeguarding the civil liberties of Americans.

16. Does the legislative history of FISA "reflect an intention that the phrase 'authorized by statute' was a reference to chapter 119 of Title 18 of the U.S. Code (title III) and to FISA itself, rather than having a broader meaning, in which case a clear indication of Congress's intent to amend or repeal it might be necessary before a court would interpret a later statute as superceding it"?[21] Do you agree with this assertion? Please explain.

The legislative history reveals no such intention to limit the scope of section 109(a) to one chapter in one part of the United States Code, even if such a reference buried in a committee report could be probative in light of the plain meaning of "authorized by statute." The legislative history focusing on chapter 119 of title 18 discussed in the CRS report you cite is directed at section 109(b), which provides an affirmative defense to law enforcement and investigative officers who conduct electronic surveillance "pursuant to a search warrant or court order" of a court of competent jurisdiction. That legislative history has *nothing* to do with whether the electronic surveillance is otherwise authorized by statute. As the legislative history makes clear, there were certain forms of electronic surveillance that potentially were prohibited by the new FISA statute that would be permitted if a court issued a warrant or order.

In any event, the assertion that in enacting FISA, Congress was attempting to limit itself—to require subsequent Congresses to jump through the formal hoop of explicitly "amending or repealing" FISA before a statute could qualify under section 109(a)—is unsustainable.

17. Have past United States Presidents employed signals intelligence of the kind authorized by President Bush after 9/11 to protect the nation during wartime? Please explain.

Presidents have intercepted enemy messages to protect the Nation during a time of war since the earliest days of the Republic. This rich history is detailed at length in the Justice Department's paper of January 19, 2006. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 14-18. In the electronic age, Presidents Wilson authorized the interception of *all* cable, telegraph, and telephone communications into and out of the United States during World War I. *See* Exec. Order No. 2604 (Apr. 28, 1917). During World War II, President Roosevelt similarly ordered the interception of *all* "telecommunications traffic" into and out of the United States. *See* Memorandum for the Secretaries of War, Navy, State, and Treasury, the Postmaster General, and the Federal Communications Commission from Franklin D. Roosevelt (Dec. 8, 1941). The Terrorist Surveillance Program, by contrast, is far more targeted and directly fulfills the President's core constitutional obligation to protect the

[21] 40 CRS Memo.

Nation from foreign attack. The Terrorist Surveillance Program targets for interception only those communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization.

18. Does the Administration's position rely, as asserted by the January 5, 2006 CRS Memorandum, on the assumptions that (1) "the power to conduct electronic surveillance for intelligence proposes is an essential aspect of military force in the same way that the capture of enemy combatants on the battlefield is a necessary incident to the conduct of military operations," and (2) the Administration considers "the battlefield' in the war on terrorism to extend beyond the area of traditional military operations to include U.S. territory"? The CRS Memorandum continues that "[b]oth assumptions have been the subject of debate."[22] Do you agree that it is debatable as to whether the United States homeland is still a target of al Qaeda?

Signals intelligence targeted at the declared enemy of the United States during an armed conflict is certainly a "fundamental and accepted incident of war." As described above, past Presidents have a long history of employing intelligence surveillance against the enemy. As detailed in the January 19th paper, the laws of war have long recognized the permissibility and necessity of conducting signals intelligence. In order to attack the enemy, it is imperative to ascertain the enemy's location and plans. In this regard, it is important to note that Congress charged the President not only with using "all necessary and appropriate force" against the enemy, but to "determine[]" who the enemy is. Fulfilling those demands requires effective intelligence.

The United States homeland is certainly still the target of al Qaeda. Indeed, as recently as December 7, 2005, Ayman al-Zawahiri stated that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). And earlier this year, Osama bin Laden warned that al Qaeda was preparing another attack on our homeland. After noting the deadly bombings his organization had committed on London and Madrid, he said that

> The delay in similar operations happening in America has not been because of failure to break through your security measures. The operations are under preparation and you *will see them in your homes* the minute they are through (with preparations), with God's permission.

Quoted at http://www.breitbart.com/news/2006/01/19/D8F7SMRH5.html (Jan. 19, 2006) (emphasis added). The threat from al Qaeda continues. Our enemies in this armed conflict have unfortunately made the United States a part of the battlefield. The attacks by al Qaeda on September 11th occurred *in the United States* and killed approximately

[22] 34 CRS Memo.

3,000 Americans—the highest single-day death toll from hostile foreign attack in the Nation's history. That al Qaeda has brought the battle to the United States cannot be the subject of reasonable debate.

CRS is also wrong to suggest that the Terrorist Surveillance Program somehow "extend[s the conflict] beyond the area of *traditional* military operations to include U.S. territory." A crucial part of any war has been protecting the United States homeland against attack by the enemy, even where the conventional warfare occurs abroad. In order to protect the Nation against domestic attack and sabotage by the enemy, Presidents Wilson and Roosevelt ordered the interception of *all* electronic communications into and out of the United States, notwithstanding the fact that—with the exception of the Japanese attacks on Pearl Harbor and at Dutch Harbor, Alaska—the bombs were dropped and the guns were fired in those wars in Europe, Asia, and Africa, not the United States. In short, engaging in intelligence surveillance of the enemy by intercepting communications into and out of the United States has been a "traditional military operation" even when the conventional war was being fought overseas. Indeed, the Supreme Court of the United States has held that the President has far more extensive powers on United States soil during a time of war. For example, the Court upheld the President's detention, trial by military commission, and execution of enemy combatants, caught attempting to commit acts of sabotage in the United States during World War II. *See Ex parte Quirin*, 317 U.S. 1 (1942).

19. Does the Administration interpret the AUMF's authorization to be contingent on the realization of "actual attacks"[23] on U.S. soil, or to be an authorization for the President to act in advance of actual attacks to prevent their occurrence?

The plain text of the Force Resolution demonstrates that Congress provided the necessary authorization for the President to exercise his solemn constitutional obligation to *prevent* further attacks on the United States. The preamble of the Force Resolution states that the United States must "exercise its rights to self-defense and [] protect United States citizens both at home and abroad." The Force Resolution recognizes the constitutional obligation of the President to protect the nation from attack: "the President has authority under the Constitution to take action *to deter and prevent* acts of international terrorism against the United States." Most clearly, the Force Resolution directly authorized the President to use "all necessary and appropriate force . . . in order *to prevent any future acts of international terrorism against the United States*" by those who perpetrated the September 11th attacks. Under the terms of the Force Resolution, not to mention common sense, the President need not wait until al Qaeda executes another "actual attack" on United States soil before taking protective action.

20. The January 5, 2006 CRS memorandum states, "To the extent that the President's executive order authorizes surveillance of persons who are suspected of merely supporting Al Qaeda or affiliated terrorist

[23] 37 CRS Memo.

organizations, it may be seen as being overly broad."[24] Does the President's executive order provide that persons "merely supporting al Qaeda" are covered? The CRS Memorandum appears to attempt to diminish the concern of those supporting al Qaeda in the U.S. What could be the consequences of the actions of a person "merely supporting al Qaeda?"

The Terrorist Surveillance Program authorizes the interception of international communications only where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The Program is *not* targeted at innocent bystanders. Actions sufficient to render someone a member or agent of al Qaeda or an affiliated terrorist organization cannot be dismissed lightly. Such actions could, in many circumstances, allow our enemy to launch additional attacks within the United States.

21. The January 5, 2006 CRS Memorandum states, "While the collection of intelligence is also an important facet of fighting a battle, it is not clear that the collection of intelligence constitutes a use of force."[25] Do you agree?

The suggestion that the collection of intelligence does not constitute a use of force for purposes of the Force Resolution is incorrect. As Justice O'Connor explained in *Hamdi*, fundamental and accepted incidents of military force constitute "an exercise of the 'necessary and appropriate force' Congress has authorized the President to use." *Hamdi*, 542 U.S. at 518 (plurality opinion). It has long been accepted that the collection of intelligence is an integral element of the use of force, just as one must aim a rifle before firing it. As Chief Justice John Marshall (who himself was an officer during the Revolutionary War) said of George Washington (a renowned master of military intelligence), "A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information . . . ." *Tatum v. Laird*, 444 F.2d 947, 952-53 (D.C. Cir. 1971) (internal quotation marks omitted), *rev'd on other grounds*, 408 U.S. 1 (1972).

In authorizing the use of force against al Qaeda, the Force Resolution undoubtedly authorizes actions that constitute necessary preparation for the use of force. For example, it undoubtedly authorized the transportation of munitions and medical supplies and even battlefield intelligence officers to Afghanistan, although the mere act of transportation might not, under the CRS memorandum's theory, itself be "a use of force." Any other reading of the Force Resolution would lead to the absurd result that the President is authorized to attack the enemy in Afghanistan, but is not authorized to transport troops and materiel to Afghanistan to do the fighting. But the authorization to use force necessarily also entails the traditional incidents of the use of force, such as transporting fighting forces. By the same token, the Force Resolution does not require the military to fight "blind," but rather necessarily authorizes it to use the fundamental

[24] *Id.*

[25] 35 CRS Memo.

tool of intelligence so it knows where and against whom to apply force, and to permit it to anticipate attacks. That is what the Terrorist Surveillance Program seeks to do. If there were any doubt on that score, it would be resolved by the fact that the Force Authorization itself indicates that the President is to "determine[]" who was responsible for the September 11th attacks in order to take action to prevent future attacks.

22. The January 5, 2006 CRS Memorandum explains that the "*Hamdi* plurality cited the Geneva Conventions and multiple authorities on the law of war to reach its conclusion that the capture of combatants is an essential part of warfare." The Memorandum then continues, "The Administration has not pointed to any authority similar to those cited by the Hamdi plurality [at 518-19] to support its proposition that signals intelligence is a fundamental aspect of combat."[26] Do you agree with the assumption made by CRS that signals intelligence is a less than conventional aspect of the conflict that would lead to its categorization as non-essential?

No. In our paper of January 19, 2006, the Department of Justice explained at length that signals intelligence has long been recognized as integral to wartime operations and authorized by the laws of war. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 14-17. To take but one example, Article 24 of the Hague Regulations of 1907 could not have been more clear: "the employment of measures necessary for obtaining information about the enemy and the country is considered permissible." *See also* Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) ("Every belligerent has a right . . . *to discover the signals of the enemy* and . . . to seek to procure information regarding the enemy through the aid of secret agents.") (emphasis added). When combined with the long history of this Nation intercepting communications into and out of the United States during time of war, as well as Supreme Court decisions recognizing the President's authority to conduct intelligence activities, *see, e.g.*, *Totten v. United States*, 92 U.S. 105, 106 (1876); *Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936), the Executive Branch has demonstrated that signals intelligence—like the detention of enemy combatants approved in *Hamdi*—unquestionably is a fundamental and accepted incident of war.

23. The January 5, 2006 CRS Memorandum states that "a presumption that the authorization [in the AUMF] extends to less conventional aspects of the conflict could unravel the fabric of *Hamdi*, especially where measures are taken within the United States."[27] Do you agree with CRS' presumption and conclusion?

No. The plurality opinion in *Hamdi* stands for the proposition that the Force Resolution authorizes the President to use the fundamental and accepted incidents of war

[26] *Id.*

[27] *Id.*

in prosecuting our armed conflict with al Qaeda. There, five Justices concluded that the Force Resolution authorized the detention of an enemy combatant *within the United States*. As demonstrated above, conducting signals intelligence against the enemy is precisely such a fundamental incident; it is *not* somehow a "less conventional aspect of conflict." Moreover, during previous wars, Presidents have used electronic surveillance of communications into and out of the United States on a scale far broader than that of the Terrorist Surveillance Program. To assert that the Force Resolution, or the successful prosecution of the armed conflict with al Qaeda, does not involve actions within the United States aimed at preventing further terrorist attacks in this country is to ignore the nature of this conflict. The United States was attacked on September 11th, not by planes launched from carriers hundreds of miles offshore, but by foreign agents who had resided within the United States for months or years. The Terrorist Surveillance Program is directed at undermining precisely that demonstrated capability of the enemy.

In determining whether the Force Resolution should be read to authorize action within the United States, it is helpful to note that, in it, Congress expressly recognized that the September 11th attacks "render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both *at home* and abroad." Force Resolution pmbl. (emphasis added). Congress affirmed that "the President has authority under the Constitution to take action to deter and prevent actions of international terrorism *against the United States*." *Id*. (emphasis added). Accordingly, Congress authorized the President "to use all necessary and appropriate force against those" associated with the attacks "in order to prevent future acts of international terrorism *against the United States*." *Id*. (emphasis added). In addition, when Congress passed the Force Resolution on September 14, 2001, the World Trade Center was still burning, combat air patrols could be heard over many American cities, and there was great concern that another attack within the United States would follow shortly.

24. Professor Tribe argues, in his January 6, 2006 letter, contrary to the Department of Justice's assertion, that *Hamdi* supports the conclusion that the AUMF cannot provide the requisite authorization by pointing to the fact that "the *Hamdi* plurality agreed 'that *indefinite* detention *for the purpose of interrogation*' even conceded enemy combatants 'is not authorized' by the AUMF. 124 S. Ct. at 2641 (emphasis added)."[28] Do you agree with Professor Tribe's argument?

No. The *Hamdi* plurality's statement does not support that argument. Five Justices (the plurality and Justice Thomas) *rejected* Hamdi's argument that, because the war on terror might continue indefinitely, the Force Resolution did not authorize his detention for the duration of the war. *Hamdi v. Rumsfeld*, 542 U.S. 507, 519-21 (2004) (plurality opinion); *id.* at 592, 594 (Thomas, J., dissenting). The plurality agreed that the laws of war generally permit the detention of enemy combatants for purposes of preventing their return to battle until the end of hostilities. *Id.* at 520. Although the plurality acknowledged that the duration of the conflict with al Qaeda may *in the future*

[28] Tribe, *supra* note 12, at 5.

raise difficult questions about the propriety of extended detentions of combatants to prevent their return to hostilities, it expressly declined to confront those questions because "that is not the situation we face as of this date." *Id*. Instead, Justice O'Connor's opinion concluded that the United States may detain enemy combatants "for the duration of these hostilities." *Id.* at 521. The plurality recognized that the laws of war and the Force Resolution do not authorize "indefinite detention *for the purpose of interrogation*," as opposed to prevent return to the conflict. *Id.* at 521 (emphasis added). The plurality based its conclusion on the lack of precedent supporting such conduct under the "law of war." *See generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, "Congress intended to authorize the President to take at least those actions permitted by the laws of war").

As noted in our January 19th paper, however, the law of war clearly supports the use of intelligence surveillance during wartime. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 14; *see*, e.g., Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) ("Every belligerent has a right . . . *to discover the signals of the enemy* and . . . to seek to procure information regarding the enemy through the aid of secret agents.") (emphasis added).

25. What legal precedents, if any, support the Administration's position that the September 14, 2001 AUMF directive to the President to use "all necessary and appropriate force"[29] against al Qaeda included the ability to authorize NSA intercepts of al Qaeda-related communications into and out of the United States?

The Administration's position is clearly supported by the Supreme Court's decision in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004). In *Hamdi*, five Justices concluded that the Force Resolution authorizes the President to use "fundamental and accepted" incidents of the use of military force in prosecuting the armed conflict against the terrorist organizations responsible for the September 11th attacks. *Id.* at 518-519; *id.* at 587 (Thomas, J., dissenting). And, as explained at length in the Department's paper of January 19, 2006, the use of signals intelligence to ascertain the identity and intentions of the enemy has long been a fundamental and accepted incident of the use of force. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 14-17. Intelligence surveillance is particularly important in the present conflict given the demonstrated willingness and ability of the enemy to blend in with the civilian population until it is ready to strike. It follows that the Force Resolution, as construed in *Hamdi*, authorizes the interception of communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization.

26. Putting aside the AUMF, can the Administration cite any legal precedents that support the President's authority to conduct searches for foreign

[29] Section 2(a).

intelligence purposes in the absence of express statutory or judicial authorization?

The President's inherent constitutional authority to conduct warrantless searches for foreign intelligence purposes has been repeatedly and consistently recognized by the courts. *See In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. Bin Laden*, 126 F. Supp.2d 264, 271-77 (S.D.N.Y. 2000). *Truong*, *Butenko*, and *Brown* all addressed pre-FISA surveillance that was conducted in the absence of any congressional or judicial authorization. Similarly, in *Bin Laden* the district court upheld the constitutionality of warrantless foreign intelligence searches of a U.S. citizen overseas, including a physical search of the individual's home. Although *In re Sealed Case* involved surveillance conducted pursuant to FISA, the court there expressly took "for granted" that the President has the inherent authority to conduct foreign intelligence searches, adding that "FISA could not encroach on the President's constitutional power." 310 F.3d at 742. Finally, as noted above, the Deputy Attorney General in the Clinton Administration testified before Congress that the President has inherent authority under the Constitution to conduct foreign intelligence searches of the private homes of U.S. citizens in the United States without a warrant, and that such warrantless searches are permissible under the Fourth Amendment. *See* Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 61, 64 (1994) (statement of Deputy Attorney General Jamie S. Gorelick).

27. On January 21, 2006, the *National Journal* purported that President Bush is "unilaterally interpret[ing] the law," constitutional or otherwise, in the "global war on terror."[30] Is this a proper characterization of the President's actions in authorizing the NSA program? What is the President's role in interpreting law?

The President is the Chief Executive of the United States, charged by the Constitution to "take Care that the Laws be faithfully executed." U.S. Const. art. II, § 3. In addition, the President takes an oath to "preserve, protect and defend the Constitution of the United States." *Id*. art. II, § 1. In order to execute the laws and defend the Constitution, the President must be able to interpret them. The interpretation of law, both statutory and constitutional, is therefore an indispensable and well established presidential function. *Cf. Bowsher v. Synar*, 478 U.S. 714, 733 (1986) ("Interpreting a law enacted by Congress to implement the legislative mandate is the very essence of 'execution' of the law."). In performing that role, the President is guided by relevant judicial precedent, and informs Congress about Executive Branch interpretations of laws through the oversight process. The President's power to interpret the laws is particularly important when he is engaged in a task—such as the direction of the operations of an armed conflict—that falls within the special and unique competence of the Executive

[30] Section 2(a).

Branch. The President's role in interpreting the laws is not, therefore, a "unilateral[]" one, but respects the roles of the other branches of government.

The Terrorist Surveillance Program is in keeping with those well established principles. It reflects authoritative judicial interpretations of the President's constitutional authority to conduct intelligence surveillance, as well as interpretations of the Force Resolution and FISA. In addition, the Administration repeatedly has briefed the leadership of the oversight committees about the Program.

28. On January 20, 2006, Senator Patrick Leahy introduced a resolution[31] and stated that he is "setting the record straight that Congress did not authorize President Bush's illegal spying program when it passed a 2001 resolution governing the use of military force in the war on terror."[32] Please explain the Administration's position of what the resolution governing the use of military force permits the President to do? Does it impose specific restrictions on the President?

The text of the Force Resolution clearly confers significant power on the President; it authorizes him to "use *all* necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks . . . in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons." (Emphasis added.) A majority of the Supreme Court has concluded that that language authorizes use of "fundamental and accepted" incidents of war. *Hamdi*, 542 U.S. at 518 (plurality opinion); *id.* at 587 (Thomas, J., dissenting). *Hamdi* indicates that actions that, by historical practice and under the laws of war, are fundamental and accepted incidents of war are encompassed within the "force" that Congress has authorized the President to use. *Cf.* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, "Congress intended to authorize the President to take at least those actions permitted by the laws of war"). Although the Force Resolution does not purport to impose specific restrictions on the President's authority, the scope of the Force Resolution is not unlimited. For example, it authorizes the use of force only against those nations, organizations, or persons that the President determines planned, authorized, committed, or aided the September 11th attacks, as well as those that harbored the guilty parties. Whatever the outer limits of the authority encompassed by the Force Resolution, however, it is clear that the Terrorist Surveillance Program—which authorizes interception only of those communications in which one party is outside the United States and for which there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization—fits comfortably within its terms.

[31] Alexis Simendinger, *The Speech – King for a War* (Jan. 21, 2006), http://nationaljournal.com/pubs/nj/ (last visited February 2, 2006).

[32] S. Res. 350, 109th Cong. (2006).

29. Does the lack of specific language in the AUMF referencing electronic surveillance undermine the Administration's contention that the AUMF provides the statutory authority for the program to be authorized by the President?

No. In *Hamdi*, five Justices of the Supreme Court concluded that the Force Resolution authorized the detention of U.S. citizens captured on the battlefield in Afghanistan, despite the fact that the resolution does not expressly mention detention. In reaching that conclusion, the plurality observed that "it is of no moment that the Force Resolution does not use specific language of detention." 542 U.S. at 519. Instead, what mattered was the fact that "detention to prevent a combatant's return to the battlefield is a fundamental incident of waging war." *Id*. So it is with signals intelligence as well. In authorizing the President to use "all necessary and appropriate force" against the parties responsible for the September 11th attacks—particularly because Congress indicated that it was for the President to "determine[]" who was responsible for the attacks—Congress necessarily authorized him to use the means necessary to determine the identity, location, and strength of the enemy. Other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force authorization resolutions that did not specifically address surveillance to permit warrantless surveillance to intercept suspected enemy communications. The language of the Force Resolution must be read against this historical backdrop. Because signals intelligence aimed at intercepting enemy communications has long been recognized as a fundamental incident of waging war, the Force Resolution authorizes that activity regardless of whether the text of the resolution uses the specific language of surveillance.

Review Process

30. On December 17, 2005, the President stated that "[t]he authorization [he] gave the National Security Agency after September the 11th helped address that problem in a way that is fully consistent with [his] constitutional responsibilities and authorities." He stated that "the activities [he] authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President."[33] This appears to explain the ongoing review of the program for compliance.

- **a. Please explain how the proposal for the program was reviewed before it was authorized and initiated.**
- **b. Who was included in this review prior to the program going into effect?**
- **c. What was the time line of the discussions that took place?**
- **d. When was the program authorized?**

[33] *Supra* note 2.

e. Was the program implemented in any capacity before receiving legal approval?

The President sought and received the advice of lawyers in the Department of Justice and elsewhere before the Program was authorized and implemented. The Program was first authorized and implemented in October 2001.

31. With regard to the ongoing review process of the NSA's activities that includes thorough review by the Justice Department and NSA's top legal officials, including NSA's general counsel and inspector general, please explain this review process, what each review constitutes, and how reviews were conducted when new individuals assumed positions previously held by others who already had been consulted. What is the process for reauthorizing the program?

General Hayden has stated that the Terrorist Surveillance Program is "overseen by the most intense oversight regime in the history of the National Security Agency," *see* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html, and is subject to extensive review in other departments as well. The oversight program includes review by lawyers at the Department of Justice and by the NSA's Office of General Counsel and Office of Inspector General. In addition, with the participation of the Office of the Director of National Intelligence and the Department of Justice, the Program is reviewed every 45 days and the President decides whether to reauthorize it. This review includes an evaluation of the Terrorist Surveillance Program's effectiveness, a thorough assessment of the current threat to the United States posed by al Qaeda, and assurances that safeguards continue to protect civil liberties.

32. To what extent were FISA judges informed of the program? Did FISA judges who were informed about the program object to it? In what manner were objections raised? How did the Administration respond to the objections, if they were raised? If a Member had problems with the program, what were they legally permitted to do?

Because communications with and the proceedings of the Foreign Intelligence Surveillance Court are classified and confidential, we cannot divulge the content of any discussions with the Foreign Intelligence Surveillance Court. We assure you, however, that the Department keeps the Foreign Intelligence Surveillance Court fully informed regarding information that is relevant to the FISA process.

33. Did any of the individuals involved in the pre-program review express concern or refuse to sign-off on the program?

a. On January 9, 2006, *Newsweek* published a story on the development of the program. The article claims that "On one day in the spring of 2004, White House chief of staff Andy Card and the then White House Counsel

Alberto Gonzales made a bedside visit to John Ashcroft, attorney general at the time, who was stricken with a rare and painful pancreatic disease, to try—without success—to get him a reverse his deputy, Acting Attorney General James Comey, who was balking at the warrantless eavesdropping."[34] Is this accurate?

b. On January 17, 2006, the *New York Times* reported that FBI officials repeatedly complained about the NSA "eavesdropping program" and believed that it was intruding upon the rights of everyday law-abiding U.S. citizens.[35] Are there documented complaints by FBI officials challenging the legality of this program at the time of its inception or throughout its activity?

c. The *Times* article claimed that Director Mueller also raised concerns about the legal rationale of the NSA program. Is this claim accurate and, if so, were Director Mueller's concerns addressed to his satisfaction?

It would be inappropriate for us to disclose any confidential and privileged internal deliberations of the Executive Branch.

34. The President in his December 17, 2005 radio address, also pointed out that the leadership and the Intelligence Committee chairs and ranking members "have been briefed more than a dozen times on this authorization and the activities conducted under it."[36] Please explain which Members of Congress were consulted, whether any expressed concern, and how those concerns were addressed. In addition, please explain how any consultations were conducted when new individuals assumed positions previously held by others who already had been consulted.

The Administration provided appropriate briefings about the Terrorist Surveillance Program to the Chairs and Ranking Members of the House and Senate Intelligence Committees and to leaders of both parties in the House and Senate. When a new Member of Congress assumed one of those positions, he or she then was given a similar briefing. As for whether any Members of Congress expressed concerns, the Attorney General testified before the Senate that, to his knowledge, of those Members of Congress who were briefed, "no one has asserted the program should be stopped."

35. Please explain what efforts the Administration has made to keep Congress informed about the terrorist surveillance program and what, if any, efforts

---

[34] Evan Thomas and Daniel Klaidman, *Full Speed Ahead, After 9/11, Bush and Cheney Pressed for More Power and Got It Now, Predictably, the Questions Begin. Behind the NSA Spying Furor*, http://www.msnbc.msn.com/id/10663996/site/newsweek (last visited February 2, 2006).

[35] *See* Lowell Bergman, Eric Lichtblau, Scott Shane, Don Van Natta Jr.; William K. Rashbaum, contributor, *Domestic Surveillance: The Program; Spy Agency Data after Sept. 11 led F.B.I. to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1.

[36] *Supra* note. 2

the President plans to undertake to ensure the Congress is fully informed about the program.

The Administration has observed and continues to observe appropriate arrangements. The arrangements have involved the leadership of the two Houses and their respective Intelligence Committees. In addition, the Administration has already briefed the new subcommittee of the Senate Select Committee on Intelligence created to oversee the Terrorist Surveillance Program and is making similar arrangements with respect to the House Permanent Select Committee on Intelligence.

36. Please explain why the Administration is only informing the Congress as a whole of the scope and nature of this program at the present time.

The briefings of the leadership of both Houses and of the Intelligence Committees were entirely consistent with governing law when dealing with exceptionally sensitive intelligence matters. The National Security Act of 1947 contemplates that the Intelligence Committees of both Houses will be appropriately notified of intelligence programs, and the Act specifically contemplates more limited disclosure in the case of exceptionally sensitive matters. Title 50 of the U.S. Code provides that the Director of National Intelligence and the heads of all departments, agencies, and other entities of the Government involved in intelligence activities shall keep the Intelligence Committees fully and currently informed of intelligence activities "[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters." 50 U.S.C. §§ 413a(a), 413b(b). It has long been the practice of both Democratic and Republican administrations to inform the Chair and Ranking Members of the Intelligence Committees about exceptionally sensitive matters. The Congressional Research Service has acknowledged that the leaders of the Intelligence Committees "over time have accepted the executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees." *See* Alfred Cumming, *Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions*, Congressional Research Service Memorandum at 10 (Jan. 18, 2006). In view of the extraordinarily sensitive nature of this intelligence activity, broader dissemination of the operational details of the Program risked compromising it.

37. On December 20, 2005, the *St. Petersburg Times* claimed that former Senator Bob Graham, who chaired the Senate Intelligence Committee at the time the Committee was briefed about the program by Vice President Cheney, said, "We were not told that there was not going to be a warrant secured and were not told that this was going to change the standard for wiretapping of U.S. citizens." [37]

[37] *Above the Law?*, ST. PETERSBURG TIMES, Dec. 20, 2005, at Al4.

a. How much detail was disclosed to the Intelligence Committee regarding the NSA program?
b. Was the level of detail disclosed consistent with what was required by law and consistent with disclosures regarding classified other program?
c. Did any Members of Congress ask for additional details?
d. What are the legal requirements or precedents that stipulate the type of information to be disclosed or withheld?

To begin with, the Terrorist Surveillance Program does *not* "change the standard for wiretapping of U.S. citizens." The Program is an exceedingly narrow one, that targets for interception only those communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization.

The Vice President of the United States has publicly stated that he personally conducted those briefings and provided a very detailed account of the Program. Senator Pat Roberts, the Chairman of the Senate Select Committee on Intelligence, stated that those who were briefed were given repeated opportunities to ask questions and express concerns until they had received all the information they wished *See* Meet the Press, transcript for Feb. 12, 2006 (*available at* http://www.msnbc.msn.com/id/11272634/). Certainly, the fact that no court order would be obtained before intercepting communications under the Terrorist Surveillance Program clearly was disclosed to members who attended these briefings.

38. The January 17, 2006 *New York Times* article also quoted an anonymous FBI agent who allegedly said that the program uncovered no active al Qaeda networks planning attacks inside the U.S.. Does the President conduct ongoing evaluations of the effectiveness of this program?[38]

As discussed in above in the response to Question 31, the President has required that the Terrorist Surveillance Program be reviewed approximately every 45 days. The purpose of those reviews is to ensure that the Program continues to remain necessary and effective in helping to safeguard the Nation against another terrorist attack. The Department is confident that the Program is helping to achieve that goal. Although we cannot fully address the Program's accomplishments without revealing classified and sensitive operational details, the statements of General Hayden and Director Mueller at the February 2d Worldwide Threat Briefing are illustrative. General Hayden stated that "the program has been successful; . . . we have learned information from this program that would not otherwise have been available" and that "[t]his information has helped detect and prevent terrorist attacks in the United States and abroad." Director Muller stated that "leads from that program have been valuable in identifying would-be terrorists in the United States, individuals who were providing material support to terrorists."

[38] *See supra* note 29.

The Surveillance Program

39. Please explain the exact scope of the terrorist surveillance program described by the President. Specifically, please explain whether the program is designed to intercept only international communications or whether it is also designed to intercept domestic communications.

a. What is the distinction?

b. **Also, please specifically describe the type of individual targeted by the program. In doing so, please explain whether the program is targeted specifically at the surveillance of individuals affiliated with al Qaeda and related terrorist organizations or whether it is broader in scope.**

The Terrorist Surveillance Program targets for interception only those communications where one party is outside of the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not target for interception wholly domestic communications.

40. On December 16, 2005, the *New York Times* claimed that President Bush "secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without court-approved warrants ordinarily required for domestic spying, according to government officials."[39]

a. Did President Bush authorize this program to search for evidence of terrorist activity or was there a more narrow purpose for this surveillance?

b. If the purpose was more narrow, please describe that purpose.

The narrow purpose of the Terrorist Surveillance Program is to create an early-warning system aimed at detecting and preventing another catastrophic al Qaeda attack on the United States. To the extent that your question about using the Program "to search for evidence" seeks to determine whether the Program is designed for conventional law enforcement purposes, that is not the purpose of the Program. The purpose of the Terrorist Surveillance Program is not to bring criminals to justice.

41. Has surveillance conducted under this program been of communications between parties, all of which were known to be located within the United States?

As we have explained above, the Terrorist Surveillance Program targets for interception only those communications where one party is outside of the United States

[39] James Risen and Eric Lichtblau, Barclay Walsh, contributor, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not target for interception wholly domestic communications.

42. If al Qaeda members purchase cell phones with U.S. domestic phone numbers, but these members are located and are placing phone calls outside the United States, would these calls be characterized as "domestic"? Does the characterization change if the call is routed domestically?

Because the question calls for the revelation of operational details about the Program, we cannot discuss it in this setting.

43. The President explained that these intercepts were related to the war on terrorism and that, "Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks."[40] Is this still true? What is the standard?

The President's explanation remains entirely correct. As explained above, the Terrorist Surveillance Program is narrowly tailored to target for interception only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof, *see Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"), and "probable cause" is the standard employed under FISA for approving applications for electronic surveillance.

44. Please explain in detail whether the terrorist surveillance program complies with the requirements of the Fourth Amendment.

The Fourth Amendment 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. v. Acton*, 515 U.S. 646, 653 (1995).

All of the federal courts of appeals to have addressed the issue have affirmed the President's inherent constitutional authority to collect foreign intelligence without a warrant. *See In re Sealed Case*, 310 F.3d at 742. Properly understood, foreign intelligence collection in general, and the Terrorist Surveillance Program in particular, fit within the "special needs" exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the Terrorist Surveillance Program does not render the activities

[40] *Supra* note 2.

unreasonable. Instead, reasonableness in this context must be assessed under a general balancing approach, "'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)). The Terrorist Surveillance Program is reasonable because the Government's interest, defending the Nation from another foreign attack in time of armed conflict, outweighs the individual privacy interests at stake, and because it seeks to intercept only communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization.

In "the criminal context," the Fourth Amendment reasonableness requirement "usually requires a showing of probable cause" and a warrant. *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). The requirement of a warrant supported by probable cause, 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, e.g.*, *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).

In particular, the Supreme Court repeatedly has made clear that in situations involving "special needs" that go beyond a routine interest in law enforcement, the warrant requirement is inapplicable. *See 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*, 531 U.S. at 330 ("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 all of the different circumstances the Court has found to qualify as "special needs" justifying warrantless searches. But one application in which the Court has found the warrant requirement inapplicable is in circumstances in which 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. One important factor in establishing "special needs" is whether the Government is responding to an emergency that goes 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 of 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 extracurricular activities at public schools for drug use, *see Vernonia*, 515 U.S. at 654-

55; *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 extracurricular activities); *Michigan Dep't of State 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 (1976) (road block near the border to check vehicles for illegal immigrants); *cf. In re Sealed Case*, 310 F.3d at 745-46 (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 general crime control. *See, e.g.*, *Ferguson v. Charleston*, 532 U.S. 67 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000).

Foreign intelligence collection, especially in the midst of an armed conflict in which the enemy 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. The Executive Branch has long maintained that collecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. *See, e.g.*, Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is inapplicable to such [foreign intelligence] searches."); *see also In re Sealed Case*, 310 F.3d 745. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like al Qaeda and affiliated terrorist organizations, including the possibility of another foreign attack on the United States. In foreign intelligence investigations, moreover, the targets of surveillance often are agents of foreign powers, including international terrorist groups, who may be specially trained in concealing their activities and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation. Even in the domestic context, the Supreme Court has recognized that there may be significant distinctions between wiretapping for ordinary law enforcement purposes and domestic national security surveillance. *See United States v. United States District Court*, 407 U.S. 297, 322 (1972) ("*Keith*") (explaining that "the focus of domestic [security] surveillance may be less

precise than that directed against more conventional types of crime" because often "the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency"); *see also United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (reading *Keith* to recognize that "the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations").

In particular, the Terrorist Surveillance Program is undertaken to prevent further devastating attacks on our Nation, and it serves the highest government purpose through means other than traditional law enforcement. The Program is designed to enable the Government to act quickly and flexibly (and with secrecy) to find agents of al Qaeda and its affiliates—international terrorist groups which have already demonstrated a capability to infiltrate American communities without being detected—in time to disrupt future terrorist attacks against the United States. As explained by the Foreign Intelligence Surveillance Court of Review, the nature of the "emergency" posed by al Qaeda "takes the matter out of the realm of ordinary crime control." *In re Sealed Case*, 310 F.3d at 746. Thus, under the "special needs" doctrine, no warrant is required by the Fourth Amendment for the Terrorist Surveillance Program.

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." *Knights*, 534 U.S. at 118-19 (quotation marks omitted); *see also Earls*, 536 U.S. at 829. The Supreme Court has found a search 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 Knights*, 534 U.S. at 118-22. Under the standard balancing of interests analysis used for gauging reasonableness, the Terrorist Surveillance Program 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 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. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests—including routine law enforcement and foreign-intelligence gathering—can overcome those interests.

On the other side of the scale here, the Government's interest in implementing the Terrorist Surveillance Program is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation in 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 (1863) ("If war be made by invasion of a foreign nation, the President is not 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).

The Government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting international communications where there is "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (Dec. 19, 2005) (statement of Attorney General Gonzales); *cf. Edmond*, 531 U.S. at 44 (noting that "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). The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. And the President has stated that the Terrorist Surveillance Program is "critical" to our national security. Press Conference of President Bush (Dec. 19, 2005). To this day, finding al Qaeda sleeper agents in the United States remains one of the preeminent concerns of the war on terrorism. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September 11th." *Id.*

Of course, because the magnitude of the Government's interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. It is thus significant for the reasonableness of the Terrorist Surveillance Program that the President has established a system under which he authorizes the surveillance only for a limited period, typically for 45 days. This process of reauthorization ensures a periodic review to evaluate whether the threat from al Qaeda 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.

Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, it is significant that the Terrorist Surveillance Program is limited to intercepting international communications where there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. This factor 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."). That consideration does not mean that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. 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 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 Terrorist Surveillance Program is targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the Program.

In sum, the Terrorist Surveillance Program is consistent with the Fourth Amendment because the warrant requirement does not apply in these circumstances, which involve both "special needs" beyond the need for ordinary law enforcement and the inherent authority of the President to conduct warrantless intelligence surveillance to obtain foreign intelligence to protect our Nation from foreign armed attack. The touchstone of the Fourth Amendment is reasonableness, and the Terrorist Surveillance Program is certainly reasonable, particularly taking into account the nature of the threat the Nation faces.

45. Throughout the Federal criminal code,[41] the statutes authorize arrests without warrants if there is "reasonable grounds to believe" that a crime has been or is about to be committed. Does this a probable cause standard translate to the NSA program? Is there case law to support this standard?

As explained above, the Terrorist Surveillance Program targets for interception only communications where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'").

46. Please explain what efforts are currently underway with respect to the terrorist surveillance program to ensure that the civil liberties and privacy

[41] *See, e.g.*, 18 U.S.C. § 3051.

of ordinary Americans are adequately protected and what additional efforts, if any, the President is considering to effectively address these issues.

As explained above, the processes for approving particular instances of surveillance under the Terrorist Surveillance Program, and for periodically reviewing the Program as a whole, are careful and thorough. Surveillance decisions are made by professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communication systems). Relying on the best available intelligence and subject to rigorous oversight, these officers, before ordering the interception of any international communications, must determine whether there is probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

In addition, the Terrorist Surveillance Program is reviewed and reauthorized at the highest levels of Government approximately every 45 days, and this process is designed to ensure that the Program will not be continued unless the al Qaeda threat to the United States continues to justify use of the Program. In making a determination to reauthorize the Program, the President relies on reviews undertaken by the Intelligence Community and Department of Justice, a strategic assessment of the continuing importance of the Program to the national security of the United States, and assurances that safeguards continue to protect civil liberties.

47. Press reports have stated that the Justice Department has opened an investigation of the leak of information regarding the highly classified NSA program.[42] Does the Department consider the unauthorized disclosure of information about this program to be a leak of classified information? Has the Department, as reported by the press, opened an investigation of the leak of this information?

The Department of Justice has initiated an investigation to determine whether the law was broken when the existence of the Terrorist Surveillance Program was leaked to the news media. If it is determined, after a careful evaluation of all the evidence, that a crime has been committed, then Department of Justice officials will have to decide whether to bring appropriate criminal charges against those responsible. Consistent with established Department of Justice practice, however, we cannot comment further on this ongoing investigation.

[42] *See, e.g., Inquiry into leak of NSA spying program launched*, CNN.com, Dec. 30, 2005, http://www.cnn.com/2005/POLITICS/12/30/nsa.leak/index.html (last visited February 3, 2006); Dan Eggan, *Justice Dept. Investigating Leak of NSA Wiretapping – Probe Seeks Source of Classified Data*, WASHINGTON POST, Dec. 31, 2005, at A1.

48. The *Washington Post* reported that "Fewer than 10 U.S. citizens or residents a year, according to an authoritative account, have aroused enough suspicion during warrantless eavesdropping to justify interception of their domestic calls, as well."[43] Are targets of the NSA surveillance program "U.S. citizens and residents," or do targets also include non-U.S. persons? Are targets of this surveillance program those who have "aroused enough suspicion" or are there other justifications for the interception? Do you agree with the premise made by the *Washington Post* that this program monitored domestic calls?

The Terrorist Surveillance Program targets communications only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. Accordingly, it is possible that the NSA has intercepted communications to which a U.S. person is a party. As we have explained, however, the Program does not target communications that are wholly domestic (i.e., those made from one point in the United States to another). In addition, as mentioned above, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

49. This article also stated that "Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human eyes and ears." And that "Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order to likeliest interest to human analysts. But intelligence officers, who test the computer judgments by listening initially to brief fragments of conversation, "wash out" most of the leads within days or weeks."[44] General Hayden, in an interview with Chris Wallace on February 5, 2006, indicated that this is not an accurate depiction of the NSA surveillance program. Is this a data-mining program, as the *Washington Post* article conveys, or is this a limited program "where NSA has already established its reasons for being interested in that specific communication"?

As General Hayden correctly indicated, the Terrorist Surveillance Program is *not* a "data-mining" program. He stated that the Terrorist Surveillance Program is not a "drift net out there where we're soaking up everyone's communications"; rather, under the Terrorist Surveillance Program, NSA targets for interception "very specific [international] communications" for which, in NSA's professional judgment, there is

---

[43] Barton Gellman, Dafna Linzer, and Carol D. Leoning, *Surveillance Net Yields Few Suspects; NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASHINGTON POST, Feb. 5, 2006, at A1.

[44] *Id.*

probable cause to believe that one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist group—people "who want to kill Americans." *See* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html.

50. On behalf of a group of organizations[45] that requested, in a January 30, 2006 letter to Chairman Sensenbrenner and Ranking Member Conyers, oversight of the NSA surveillance program, please respond to the following:

a. Is the NSA surveillance program a single program, which operates under a single authorization? What is the scope and/or nature of the program(s)?
b. What are the criteria and triggers for collection and/or analysis of information? How do these criteria and triggers differ from those in effect prior to September 11, 2001?
c. Were laws violated and, if so, who bears responsibility?
d. What information is obtained through this program? Is it shared with other agencies? Once obtained, how is it used and/or stored, whether by NSA or other agencies?

We are able to address only the Terrorist Surveillance Program. We cannot address the operational details of the Program or any other sensitive intelligence activities. The Terrorist Surveillance Program allows the NSA to intercept only a narrow range of communications. Communications are not targeted for interception under the Program unless one party is outside the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. FISA also employs a probable cause standard (specifically, whether there is "probable cause to believe" that the target of the surveillance is an agent of a foreign power). Among the advantages offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination and how many layers of review will occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communication systems), relying on the best available intelligence and with appropriate and rigorous oversight, make the

[45] American–Arab Anti-Discrimination Committee, American Civil Liberties Union, American Friends Service Committee, American Progress Action Fund, Amnesty International USA, Arab Community Center for Economic and Social Services, Bill of Rights Defense Committee, Center for Democracy and Technology, Center for Financial Privacy and Human Rights, Center for National Security Studies, Common Cause, Constitution Project, Darfur Alert Coalition, Democrats.com, Electronic Frontier Foundation, Electronic Privacy Information Center, Fairfax County Privacy Council, First Amendment Fund, Federation of American Scientists, Friends Committee on National Legislation, Hate Free Zone Washington, League of United Latin American Citizens, Liberty Coalition, MoveOn.org Political Action, Muslim Advocates, Muslin Public Affairs Council, National Association of Criminal Defense Lawyers, National Committee Against Repressive Legislation, National Lawyers Guild – National Office, National Network for Arab American Communities, National Security Whistleblowers Coalition, Open Society Policy Center, Patriots to Restore Checks and Balances, People for the American Way, Privacy Activism, Republican Liberty Caucus, Rutherford Institute, United for Peace and Justice, U.S. Bill of Rights Foundation, The Multiracial Activist, World Privacy Forum.

decisions about which communications should be intercepted. By contrast, because FISA requires the Attorney General to "reasonably determine[]" that "the factual basis for issuance of" a FISA order exists at the time he approves an emergency authorization, *see* 50 U.S.C. § 1805(f)(2), as a practical matter, it is necessary for NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General to review a matter before even emergency surveillance would begin. As noted above, great care must be exercised in reviewing requests for emergency surveillance, because if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, there is a risk that the court would disclose the surveillance to U.S. persons whose communications were intercepted. *See* 50 U.S.C. § 1806(j).

After a thorough review, the Department of Justice has concluded that the Terrorist Surveillance Program is lawful, because it represents a legitimate use of the President's long-recognized inherent constitutional authority to engage in warrantless surveillance in order to gather foreign intelligence information, an authority that was confirmed and supplemented by Congress when it enacted the Force Resolution. In addition, the Force Resolution provides the statutory authorization necessary to satisfy the requirements of section 109 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1809(a)(1).

We cannot, in this setting, answer questions about how the information obtained through the Terrorist Surveillance Program is used and stored without revealing operational details about the Program. We note, however, that General Hayden has stated that information from the Program "has helped detect and prevent terrorist attacks in the United States and abroad." Procedures are in place, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

51. Finally, please explain whether you believe Congress should amend FISA to provide the president with the necessary authority to conduct the terrorist surveillance program. If the answer to this question is yes, please explain what amendments to the FISA legislation may be needed. If the answer to this question is no, please explain how Congress may effectively evaluate or conduct oversight of the program.

The Administration believes that it is unnecessary to amend FISA to accommodate the Terrorist Surveillance Program. The Administration will, of course, work with Congress and evaluate any proposals for improving FISA.

RESPONSES TO JOINT QUESTIONS FROM HOUSE JUDICIARY COMMITTEE MINORITY MEMBERS

Targets of Surveillance

1. Approximately how many persons located in the US have been targets of government intelligence activity under the warrantless surveillance program?

The National Security Agency ("NSA") electronic surveillance activities confirmed by the President involve targeting for interception by the NSA of communications where one party is outside the United States and there is probable cause ("reasonable grounds") to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program" or the "Program"). Operational details about the scope of the Terrorist Surveillance Program are classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the scope of the Program could compromise its value by facilitating terrorists' attempts to evade it. We note, however, that consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

2. What criteria is used by NSA staff to determine whether one party to the communication is a person working in support of al Qaeda?

Under the Terrorist Surveillance Program, decisions about what communications to intercept are made by professional intelligence officers at the NSA who are experts on al Qaeda and its tactics, including its use of communications systems. Relying on the best available intelligence and subject to appropriate and rigorous oversight by the NSA Inspector General and General Counsel, among others, the NSA determines whether one party is outside of the United States and whether there is probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

3. Is the internal standard used to decide whether to monitor the communications of a person in the United States under the Program identical to the FlSA standard? In other words, before someone's communications are targeted for interception, does someone determine that there is probable cause to believe the target is knowingly conspiring with a foreign terrorist?

The Terrorist Surveillance Program targets communications only where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated

. . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). FISA also employs a probable cause standard (specifically, whether there is "probable cause to believe" that the target of the surveillance is an agent of a foreign power). *See* 50 U.S.C. § 1805(a)(3).

4. Once the NSA decides to monitor the communications of a person in the United States, do they also target and monitor the communications of any person in the United States who communicates with the original target? If so, does someone first determine whether the second target is knowingly conspiring with a foreign terrorist?

As set forth above, communications are targeted for interception under the Terrorist Surveillance Program only if one party is outside the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

Scope of NSA Program

5. How many hours and dollars have been spent searching or seizing the phone calls or emails of people in the US, and how much of this has been spent on people who have never been charged with any crime?

Operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. As noted above, consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

6. How many people in the US have been referred to the FBI for further inquiry or investigation? How many people whose emails or phone calls have been monitored have never been referred to the FBI?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

7. Are the names, phone numbers, or email addresses of persons in the United States who have had their communications monitored as part of the Program been included on any watch lists?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

Telecommunications Companies

8. Telecommunications companies and Internet Service Providers ("ISPs") are protected from criminal and civil liability if they are provided a court order from the FlSA court or criminal court or if a high-ranking DOJ official has certified in writing that "No warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." Has anyone at the Justice Department provided any telephone companies or ISPs with these certifications in the course of implementing the NSA's program?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore we cannot confirm or deny operational details of the program in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

9. Which telecommunications firms have opened American communications arteries to the NSA without a warrant?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore we cannot confirm or deny operational details of the program in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

Use of Information

10. To what extent has information collected included details of the targets' personal lives or political views, and has such information been immediately destroyed? Have intelligence agencies taken any actions beyond surveillance with regard to such individuals?

The purpose of the Terrorist Surveillance Program is to protect the Nation from foreign attack by detecting and preventing plots by a declared enemy of the United States that has already killed thousands of innocent civilians in the single deadliest foreign attack on U.S. soil in the Nation's history. In order to advance that end while simultaneously protecting civil liberties, procedures are in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

11. Was evidence obtained from the NSA classified surveillance program subsequently used to obtain a warrant from the FlSA court? If so, how many times has this occurred?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Nor can we disclose the content of classified and sensitive communications and pleadings filed with the Foreign Intelligence Surveillance Court.

12. What is done with the information collected from the warrantless surveillance program that ends up not being useful for law enforcement or security purposes?

As indicated above, procedures are in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons. Those guidelines are designed to ensure that the Terrorist Surveillance Program is conducted in a manner consistent with preserving civil liberties.

13. Other than the President, what individuals at the White House are briefed on the program, and how often are they briefed?

The Terrorist Surveillance Program remains classified and highly sensitive. In general, the identity of individuals who have been briefed into the Program is also classified. We have previously explained, however, that the President sought legal advice prior to authorizing the Terrorist Surveillance Program and was advised that it is lawful, and that the Program has been reviewed by lawyers at the Department of Justice (including the Attorney General), by lawyers at the NSA, and by the Counsel to the President. Since 2001, the Program has been reviewed multiple times by different

counsel. Although the President is responsible for reauthorizing the Program, his determination to do so is based on reviews undertaken by the Intelligence Community and Department of Justice, a strategic assessment of the continuing importance of the Program to the national security of the United States, and assurances that safeguards continue to protect civil liberties. That process requires certain individuals to be cleared to receive classified and sensitive information about the Program.

14. When was James Baker read into the Program?

Please refer to the answer to question 13.

15. Who at the Department of Justice was informed of the Program? When?

Please refer to the answer to question 13.

16. When was the Solicitor General's office and the Deputy Attorney General's office informed of the program?

Please refer to the answer to question 13.

17. Does the Attorney General personally approve or authorize each interception of a United States person's communication? If not, who approves each interception?

As explained above, under the Terrorist Surveillance Program, professional intelligence officers at NSA, who are experts on al Qaeda and its tactics (including its use of communications systems), make the decisions about which international communications should be intercepted. Relying on the best available intelligence and subject to appropriate and rigorous oversight, those officers determine whether there is probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. In addition, the NSA, the Department of Justice, and the Office of the Director of National Intelligence conduct oversight of the Terrorist Surveillance Program through, for example, the reauthorization process.

18. Does anyone independent of the NSA check persons in the US whose phone calls or emails are searched or seized to make sure that they are not being targeted based on their political opinions?

General Hayden has stated that the Terrorist Surveillance Program is "overseen by the most intense oversight regime in the history of the National Security Agency," *see* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html, and is subject to extensive review in other departments as well. The oversight program includes review at the National Security Agency (by both the Office of General Counsel and Office of Inspector General) and the Department of Justice. In addition, with the participation of the Office of the Director of National Intelligence and the Department of Justice, the Program is reviewed

every 45 days, and the President decides whether to reauthorize it. This review includes an evaluation of the Terrorist Surveillance Program's effectiveness, a thorough assessment of the current threat to the United States posed by al Qaeda, and assurances that safeguards continue to protect civil liberties.

Minimization Procedure

19. Executive Order 12,333[] provides that intelligence agencies are only authorized to collect information on US persons consistent with the provisions of that Executive Order and procedures established by the head of the agency and approved the Attorney General. (Sec. 2.3). What minimization procedures are in effect concerning information gathered by the NSA concerning persons in the US?

Procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons. NSA applies minimization procedures that are appropriate and approved for the activity at issue. For example, special minimization procedures, approved by the Foreign Intelligence Surveillance Court, govern NSA handling of U.S. person information acquired pursuant to FISA-authorization surveillance. Department of Defense Regulation 5240.1-R (and its classified annex) are the guidelines approved by the Attorney General that are referred to in Executive Order 12333. Those guidelines govern NSA's handling of U.S. person information. United States Signals Intelligence Directive 18 provides more detailed guidance on the latter.

20. Has United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures," July 27, 1993, applicable to the NSA, been changed since January 2001? Is it still in effect? Does that Directive, as amended or not, apply to all surveillance being undertaken by the NSA of persons inside the US outside of the procedures set forth in FISA?

United States Signals Intelligence Directive 18 has not been changed since January 2001 and is still in effect. As indicated above, procedures are in place under the Terrorist Surveillance Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

21. When were the minimization procedures last changed? Did the Attorney General approve those changes? When?

Executive Order 12333 calls for Attorney General-approved procedures for the collection, retention, and dissemination of information concerning U.S. persons. The Secretary of Defense issued the current version of these procedures in December 1981

applicable to all Department of Defense ("DoD") intelligence agencies. The Attorney General signed those procedures in October 1982. A classified annex to those procedures dealing specifically with signals intelligence was promulgated by the Deputy Secretary of Defense in April 1988 and approved by the Attorney General in May 1988. NSA has internal procedures derivative of those authorities that were last updated in 1993. The annex that specifically governs FISA procedures was modified, with Attorney General Reno's approval, in 1997.

22. When was the last time you supplied any Member of the House Judiciary Committee or any Committee of the Congress a copy of such minimization procedures?

NSA has briefed intelligence committees of both Houses extensively on minimization procedures over the past several years. NSA can determine from available records only that NSA provided Senate Select Committee on Intelligence staff DoD Regulation 5240.1-R and its classified annex in January 2006 and both USSID 18 and DoD Regulation 5420.1-R and its annex in July 2005. NSA's records do not indicate when a copy of those materials was last provided to the House Permanent Select Committee on Intelligence. However, it is important to note that much of this material is freely available. USSID 18, July 27, 1993, has been made publicly available in redacted form (*see, e.g.*, www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm). In addition, DoD Regulation 5240.1-R, December 1982 (but not its annex) has been declassified and made publicly available (*see, e.g.*, http://cryptome.org/dod5240-1r.htm).

Concerns About the NSA Program from Within the Administration

23. How many federal employees have expressed concerns about or objections to this program and what has been done regarding those employees of the NSA or other federal agencies or in response?

It would be inappropriate for us to disclose any confidential internal deliberations of the Executive Branch. The long-recognized confidentiality protections afforded Executive Branch communications are designed to encourage candid advice from Executive Branch lawyers and officers, and subjecting such advice to disclosure would chill those deliberations. The General Counsel and Inspector General of the NSA oversee the NSA's implementation of the Terrorist Surveillance Program. We note that there are procedures in place under the Intelligence Community Whistleblower Protection Act of 1998 that permit employees concerned about the legality of intelligence programs to report their concerns to the inspectors general of intelligence agencies and thence to Congress.

24. Why was the NSA program suspended in 2004?

The Terrorist Surveillance Program described by the President has never been suspended; it has been in operation since its inception in October 2001. Indeed, the President explained that he intends to reauthorize that Program as long as the threat posed

by al Qaeda and its allies justifies it. Beyond this, we cannot discuss the operational details or history of the Terrorist Surveillance Program. Nor can we divulge the internal deliberations of the Executive Branch.

Presidential Claim of Inherent Authority

25. What is the limiting principle of the President's claimed inherent authority as commander-in-chief? For example, does this interpretation of the law authorize the opening of first-class mail of U.S. citizens under the DOJ's interpretation, and if not, why not?

The Terrorist Surveillance Program intercepts only communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not include the opening of first-class United States mail. There is a long history of Presidents, including Woodrow Wilson and Franklin Roosevelt, authorizing the interception of international electronic communications during times of armed conflict as an exercise of the President's inherent authority under the Constitution and pursuant to general force authorization resolutions. Whether the President's authority under the Constitution would permit the interception of mail would require a different legal analysis. In light of the strictly limited nature of the Terrorist Surveillance Program, we do not think it a useful or a practical exercise to engage in speculation about the limits of the President's authority as Commander in Chief. *Cf. Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("The actual art of governing under our Constitution does not and cannot conform to judicial definitions of the power of any of its branches based on isolated clauses or even single Articles torn from context.").

26. Under the Administration's legal interpretation, does the President have the authority to wiretap Americans' domestic calls and emails under his inherent constitutional power and the AUMF, if he feels it involves al Qaeda activity?

The Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. There is a long history of Presidents authorizing the interception of *international* electronic communications during a time of armed conflict. President Wilson, for example, relying only on his constitutional powers and a general congressional authorization for use of force, authorized the interception of *all* telephone, telegraph, and cable communications into and out of the United States during World War I. *See* Exec. Order 2604 (Apr. 28, 1917). Similarly, President Roosevelt authorized the interception of "*all . . . telecommunications traffic* in and out of the United States." As explained in the Justice Department's paper of January 19, 2006, that historical foundation lends significant support to the President's authority to undertake the Terrorist Surveillance Program under the AUMF and the Constitution; indeed, the Program is much narrower than the interceptions authorized by either President Wilson or President

Roosevelt. Interception of the content of domestic communications would present a different legal question.

Authorization for Use of Military Force (AUMF)

27. When did the Administration and DOJ decide that the Authorization for Use of Military Force (AUMF) granted the Administration the power to create the NSA program?

The Department has reviewed the legality of the Terrorist Surveillance Program on multiple occasions. We cannot discuss the operational details or history of the Terrorist Surveillance Program.

28. Are there any other actions under the AUMF that, without the President's inherent constitutional power, would not be permitted because of the FlSA statute? Are there any programs currently being used like that?

We are not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program, though our inability to respond should not be taken to suggest that there are such activities. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

29. Under the Administration's interpretation of AUMF, has the President ever invoked his authority as commander-in-chief through either secret order or directive other than NSA surveillance?

As stated above, we are not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program, though our inability to respond should not be taken to suggest that there are such activities. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

30. How do you reconcile the Attorney General's statement that Congress would not have granted the Executive such authority and at the same time, contend that this authority is something that Congress intended to give under the AUMF?

We understand your question to be a reference to a statement the Attorney General made on December 19, 2005. As the Attorney General clarified both later in the same December 19th briefing and on December 21, 2005, it is not the case that the Administration declined to seek a specific authorization of the Terrorist Surveillance Program because we believed Congress would not authorize it. *See* Remarks by

Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act, *available at* http://www.dhs.gov/dhspublic/display?content=5285. Rather, as the Attorney General testified before the Senate on February 6, 2006, the consensus view in discussions with Members of Congress was that it was unlikely, if not impossible, that more specific legislation could be enacted without compromising the Terrorist Surveillance Program by disclosing operational details, limitations, and capabilities to our enemies. Such disclosures would necessarily have compromised our national security.

Foreign Intelligence Surveillance Act (FISA)

31. When did the Administration reach the conclusion that FISA did not have to be followed to use the NSA program?

Before answering this question, we note that the Department's legal analysis assumes, solely for purposes of that analysis, that the targeted interception of international communications authorized under the President's Terrorist Surveillance Program would constitute "electronic surveillance" as defined in FISA. As noted in our January 19th paper, we cannot confirm whether that is actually the case without disclosing sensitive classified information.

As explained at length in the Justice Department's paper of January 19, 2006, the Terrorist Surveillance Program is completely consistent with FISA. FISA itself includes an exception for surveillance "authorized by statute," 50 U.S.C. § 1809(a). In light of the decision in *Hamdi v. Rumsfeld* that the AUMF authorizes the President to undertake fundamental and accepted incidents of war and the long history demonstrating that signals intelligence against the enemy is such a fundamental incident of war, the AUMF is a statute that authorizes intelligence surveillance against members and agents of al Qaeda and affiliated terrorist organizations and thereby satisfies FISA.

The President was advised that the Terrorist Surveillance Program was lawful before he first authorized it in October 2001.

32. Did the increasing number of modified and rejected requests for FISA warrants since 2001 implicate the Administration's determination to bypass FISA?

As explained above, the Terrorist Surveillance Program does not "bypass FISA."

The determination to implement the Terrorist Surveillance Program was made based on the advice of intelligence experts that the Nation needed an early warning system, one that could help detect and prevent another catastrophic al Qaeda attack. The President authorized the Terrorist Surveillance Program because it offers the speed and agility required to defend the United States against further terrorist attacks by al Qaeda and affiliated terrorist organizations. Among the advantages offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination

and how many layers of review will occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communications systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. By contrast, because FISA requires the Attorney General to "reasonably determine[]" that "the factual basis for issuance of" a FISA order exists at the time he approves an emergency authorization, *see* 50 U.S.C. § 1805(f)(2), as a practical matter, it is necessary for NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General to review a matter before even emergency surveillance would begin. Great care must be exercised in reviewing requests for emergency surveillance because of the risks involved. Among other things, if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, there is a risk that the court would disclose the surveillance to U.S. persons whose communications were intercepted, *see* 50 U.S.C. § 1806(j), potentially compromising ongoing intelligence efforts. In the narrow context of defending the Nation in this congressionally authorized armed conflict with al Qaeda, we must allow these highly trained intelligence professionals to use their skills and knowledge to protect us.

33. Do you know of any other President who has authorized warrantless wiretaps outside of FlSA since FlSA was passed in 1978? If so, please explain.

The laws of the United States, both before and after FISA's enactment, have long permitted various forms of foreign intelligence surveillance, including the use of wiretaps, outside the procedures of FISA. If the question is limited to "electronic surveillance" as defined by FISA, however, we are unaware of such authorizations.

34. In a press briefing on December 19, 2005, General Hayden stated that the NSA was using a subtly softer trigger which precluded going to the FISA court. What exactly constitutes this softer trigger?

As noted above, the "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). FISA also employs a probable cause standard (specifically, whether there is "probable cause to believe" that the target of the surveillance is an agent of a foreign power). *See* 50 U.S.C. § 1805(a)(3). The relevant distinction between the two methods—and the critical advantage offered by the Terrorist Surveillance Program compared to FISA—is the greater speed and agility it offers.

35. How many FISA judges were informed of the warrantless surveillance program?

The Terrorist Surveillance Program remains classified and sensitive. In general, the identity of individuals who have been briefed into the Program is also classified. In addition, we cannot disclose the content of our discussions with the Foreign Intelligence

Surveillance Court. We assure you, however, that the Department keeps the Foreign Intelligence Surveillance Court fully informed regarding information that is relevant to the FISA process.

36. Was any judge on the FISA court of review informed of the NSA program as part of the briefing of the 2002 appellate case, *In re Sealed Case*? Were any of the lawyers on that case read into the program? How many?

As we noted above, the identity of individuals who have been briefed into the Terrorist Surveillance Program is generally classified. We note, however, that *In re Sealed Case*, 310 F.3d 717 (For. Int. Surv. Ct. Rev. 2002), involved whether the FISA Court had statutory or constitutional authority to place restrictions on interaction of criminal prosecutors and foreign intelligence investigators as a condition for granting surveillance orders. The Terrorist Surveillance Program would not have been relevant to the question before the court in that case.

37. Are there currently any plans to take the entire NSA program to the FISA Court within the broad parameters of what is reasonable and constitutional and ask the FlSA Court to approve it or disapprove it? If not, why not?

It would be inappropriate to discuss here future plans for seeking any particular order from the Foreign Intelligence Surveillance Court, which could involve both privileged internal Executive Branch communications and deliberations and classified and sensitive court filings. The Department has, however, sought to use the FISA process wherever possible, and we will continue to consider all lawful options.

38. What aspects of FISA are too burdensome for the Administration to comply with? Why did the Administration fail to utilize the emergency provision of FISA?

As noted above, the determination was made, based on the advice of intelligence experts, that the Nation needed an early warning system to help detect and prevent another catastrophic al Qaeda attack. Speed and agility are critical in this context. It would be an unjustifiable lapse if al Qaeda electronic communications were used to coordinate another deadly attack on America, but the communications were not intercepted in time because of the delay that traditional FISA procedures require.

The emergency authorization provision in FISA, which allows 72 hours of surveillance without obtaining a court order, does not—as many believe—allow the Government to undertake surveillance immediately. Rather, in order to authorize emergency surveillance under FISA, the Attorney General first must personally "determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists." 50 U.S.C. § 1805(f). FISA requires the Attorney General to determine that this condition is satisfied *in advance* of authorizing the surveillance to begin. The process needed to make that determination, in turn, can take time. Section 106(j) of FISA, 50 U.S.C. § 1806(j), provides that if a court later declines to authorize an

interception that previously was authorized by the Attorney General under the so-called "emergency" exception to FISA, it may order disclosures about the surveillance to U.S. persons whose communications were intercepted. Thus, using the "emergency" exception poses a risk that surveillance activities will be subject to public disclosure. To reduce that risk, the Attorney General follows a multi-layered procedure before authorizing interception under the "emergency" exception to help to ensure that any eventual application will be approved by the Foreign Intelligence Surveillance Court. That process ordinarily entails review by intelligence officers at the NSA, NSA attorneys, and Department of Justice attorneys, each of whom must be satisfied that the standards have been met before the matter proceeds to the next group for review. Compared to that multilayered process, the Terrorist Surveillance Program affords a critical advantage in terms of speed and agility.

Miscellaneous

39. According to the Administration, a line NSA analyst rather than an independent judge determines whether or not an intrusion into a[] citizen's privacy is reasonable. Do you think that there are appropriate checks and balances under this framework?

Yes. As noted earlier, General Hayden has stated that the Terrorist Surveillance Program is "overseen by the most intense oversight regime in the history of the National Security Agency," *see* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html, and is subject to extensive review in other departments as well. Please refer to the answer to question 18 for further information about the considerable privacy protections that are built into the Program.

40. Have any purely domestic calls intercepted through the NSA program? What happens if such calls are intercepted, to the information and the responsible employee?

The Terrorist Surveillance Program targets for interception only those communications where one party is outside of the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not target for interception wholly domestic communications (*i.e.*, communications which both originate and terminate within the United States). There are procedures in place to avoid the interception of domestic calls. In addition, as mentioned above, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

41. Is the NSA engaged in keyword analysis or pattern analysis of purely domestic communications?

The Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. It would be inappropriate to discuss in this setting the existence (or non-existence) of specific intelligence activities or the operations of any such activities other than the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

42. Is the NSA engaged in keyword analysis or pattern analysis of the communications of people in the United States who call or email overseas?

As noted above, the Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. It would be inappropriate to discuss in this setting the existence (or non-existence) of specific intelligence activities or the operations of any such activities other than the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

43. Has information obtained through warrantless NSA interceptions been used in any criminal prosecutions?

The purpose of the Terrorist Surveillance Program is not to bring criminals to justice. Instead, the Program is directed at protecting the Nation from foreign attack by detecting and preventing plots by a declared enemy of the United States. Because the Program is directed at a "special need, beyond the normal need for law enforcement," the warrant requirement of the Fourth Amendment does not apply. *See*, *e.g.*, *Vernonia School Dist. v. Acton*, 515 U.S. 646, 653 (1995). Because collecting foreign intelligence information without a warrant does not violate the Fourth Amendment and because the Terrorist Surveillance Program is lawful, there appears to be no legal barrier against introducing this evidence in a criminal prosecution. *See* 50 U.S.C. § 1806(f), (g). Past experience outside the context of the Terrorist Surveillance Program indicates, however, that operational considerations, such as the potential for disclosing classified information, must be considered in using intelligence information in criminal trials.

44. Are their any plans by the Bush administration to inform those US individuals whose phone calls or emails were searched or seized but they have been cleared of any wrongdoing?

As explained above, the Terrorist Surveillance Program is subject to rigorous oversight to protect privacy interests. In addition, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

45. Are any communications between attorneys and their clients or doctors and patients being captured?

The Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. Although the Program does not specifically target the communications of attorneys or physicians, calls involving such persons would not be categorically excluded from interception if they met these criteria. As mentioned above, however, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.