U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 24, 2006

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This responds to your letter, dated February 13, 2006, transmitting questions for the record posed to Attorney General Gonzales following his appearance before the Senate Committee on the Judiciary on February 6, 2006. The subject of the hearing was, "Wartime Executive Power and the National Security Agency's Surveillance Authority."

The enclosed document responds to the 35 combined Minority questions for the record. We can assure you we are continuing to work on additional answers to questions submitted by individual Committee Senators.

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 Patrick J. Leahy
Ranking Minority Member

"Wartime Executive Power
And The National Security Agency's Surveillance Authority"
Hearing Before The Senate Committee On The Judiciary
Written Questions From All Democratic Senators

1. **On January 27, 2006, members of this Committee wrote to you and asked that you provide relevant information and documents in advance of this hearing, including formal legal opinions of the Office of Legal Counsel ("OLC") and contemporaneous communications regarding the 2001 Authorization for Use of Military Force ("AUMF"). Please provide those materials with your answers to these questions.**

The first item in the January 27th letter asks for "communications from the Administration to Congress during the period September 11 through September 14, 2001," relating to language to be included in the Authorization for Use of Military Force ("Force Resolution") and the Administration's understanding of that language. Any such communications would presumably be in the possession of Congress. We have not identified any Department of Justice documents reflecting such communications.

You have also requested "all documents that are or reflect internal Administration communications during" the same period regarding the meaning of the language being considered for inclusion in the Force Resolution. It would be inappropriate for us to reveal the confidential and privileged internal deliberations of the Executive Branch.

You have also requested "copies of all memoranda and legal opinions rendered by the Department of Justice during the past 30 years that address the constitutionality of government practices and procedures with respect to electronic surveillance." That is potentially an extraordinarily broad request, both because of the length of the period covered (which would encompass a period before enactment of the Foreign Intelligence Surveillance Act of 1978 ("FISA")) and the sweeping terms of the request: the reference to "memoranda" could include hundreds or thousands of informal memoranda written in individual cases between 1976 and the present that are in the files of the various litigating branches of the Department. We understand your request to seek only formal memoranda and legal opinions issued by the Attorney General or the Office of Legal Counsel ("OLC") during that time involving constitutional issues arising from the interception of electronic communications or wiretapping. Many such opinions and memoranda have been published and are readily available through online databases or the Office of Legal Counsel website. In addition, some opinions responsive to your request previously have been released in response to past requests under the Freedom of Information Act ("FOIA"). Citations to relevant opinions are set forth in the margin.[1]

---

[1] Memorandum for Frances Fragos Townsend, Counsel, Office of Intelligence Policy and Review, from Randolph D. Moss, Assistant Attorney General, Office of Legal Counsel, *Re: Sharing Title III Electronic Surveillance Material with the Intelligence Community* (Oct. 17, 2000), *available at* http://www.usdoj.gov/olc/titleIIIfinal.htm; *Bureau of Prisons Disclosure of Recorded Inmate Conversations*, 21 Op. O.L.C. 11 (Jan.

Copies of unpublished opinions that do not reflect the deliberative process, or that are otherwise appropriate for release, will be provided to you in response to this request. Some more recent memoranda and opinions, though unclassified, reflect the deliberative process and are privileged, and therefore are not appropriate for release. At the time they are issued, most OLC opinions consist of confidential legal advice for senior Executive Branch officials. Maintaining the confidentiality of OLC opinions often is necessary to preserve the deliberative process of decisionmaking within the Executive Branch and attorney-client relationships between OLC and other executive offices and to avoid interference with federal law enforcement efforts.

Your request appears to seek internal memoranda addressing the National Security Agency ("NSA") electronic surveillance activities confirmed by the President. Those activities 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"). Any written legal opinions that the Department may have produced regarding the Terrorist Surveillance Program would constitute the confidential internal deliberations of the Executive Branch, and it would be inappropriate for us to reveal them. In addition, the release of any document discussing the operational details of this

---

14, 1997); *Fourth Amendment Implications of Military Use of Forward Looking Infrared Radars Technology for Civilian Law Enforcement*, 16 Op. O.L.C. 41 (Mar. 4, 1992); *Military Use of Infrared Radars Technology to Assist Civilian Law Enforcement Agencies*, 15 Op. O.L.C. 36 (Feb. 19, 1991); *Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Law Enforcement Activities*, 13 Op. O.L.C. 163 (June 21, 1989); *Applicability of Fourth Amendment to Use of Beepers in Tracking Bank Robbery Bait Money*, 10 Op. O.L.C. 138 (Dec. 5, 1986); *Presidential Power Concerning Diplomatic Agents and Staff of the Iranian Mission*, 4A Op. O.L.C. 174 (Jan. 8, 1980); *Foreign Intelligence Surveillance Act (50 U.S.C. § 1801)—Interception of Radio Communication—Constitutional Law—Fourth Amendment—Privacy*, 3 Op. O.L.C. 240 (May 29, 1979); *Constitutional Law—Fourth Amendment—Interception of Oral Communications—Legality of Television Surveillance in Government Offices*, 3 Op. O.L.C. 64 (Feb. 2, 1979); *National Security Mail Covers—Constitutional Challenge—Federal Bureau of Investigation (39 CFR 233.2(d)(2)(ii))*, 2 Op. O.L.C. 290 (Dec. 15, 1978); *Intelligence—Warrantless Electronic Surveillance—Common Carriers (18 U.S.C. §§ 2510-2520, 47 U.S.C. § 605)*, 2 Op. O.L.C. 123 (June 5, 1978); *Warrantless Foreign Intelligence Surveillance—Use of Television—Beepers*, 2 Op. O.L.C. 14 (Jan. 25, 1978). The following opinions previously have been released in response to past FOIA requests: Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, Office of Legal Counsel, *Re: Standards for Searches under the Foreign Intelligence Surveillance Act* (Feb. 14, 1995); Memorandum for Anthony A. Lapham, General Counsel, Central Intelligence Agency, from John M. Harmon, Assistant Attorney General, Office of Legal Counsel, *Re: MKULTRA Drug-testing Program* (July 17, 1978). Copies of those two opinions are attached.

highly classified and sensitive program would risk compromising the Program and could help terrorists avoid detection. As you know, on January 19, 2006, the Department of Justice released a 42-page paper setting out a comprehensive explanation of the legal authorities supporting the Program. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006). That paper reflects the substance of the Department's legal analysis of the Terrorist Surveillance Program.

Finally, you also have requested "any documents by which the President has, prior to and after September 11, 2001, authorized the NSA surveillance programs, including all underlying legal opinions authored by the White House." Such documents would reflect sensitive operational details of the program, and any such legal opinions would constitute confidential internal deliberations of the Executive Branch. Accordingly, it would be inappropriate to release such documents.

2. **Since September 11, 2001, how many OLC memoranda or opinions have discussed the authority of the President to take or authorize action under either the AUMF or the Commander-in-Chief power, or both, that one could argue would otherwise be prohibited or restricted by another statute? Will you provide copies of those memoranda or opinions to the Committee? If not, please provide the titles and dates of those memoranda and opinions.**

Any such opinions would constitute the confidential legal advice of the Executive Branch and would reflect the deliberative process. We are not able to discuss the contents of confidential legal advice.

3. **When did the President first authorize warrantless electronic surveillance of U.S. persons in the United States outside the parameters of the Foreign Intelligence Surveillance Act ("FISA")? What form did that authorization take?**

As explained in the January 19th paper, the Terrorist Surveillance Program is not "outside the parameters of [FISA]." Rather, FISA contemplates that Congress may enact a subsequent statute, such as the Force Resolution, that authorizes the President to conduct electronic surveillance without following the specific procedures of FISA.

The President first authorized the Terrorist Surveillance Program in October 2001.

4. **When did the NSA commence activities under this program?**

The NSA commenced the Terrorist Surveillance Program soon after the President authorized it in October 2001.

5. **When did the Administration first conclude that the AUMF authorized warrantless electronic surveillance of U.S. persons in the United States?**

What contemporaneous evidence supports your answer, and will you provide it to the Committee? What legal objections were raised to that theory and by whom?

The Department has reviewed the legality of the Terrorist Surveillance Program on multiple occasions. Your questions regarding the content of confidential Executive Branch legal advice, the identity of those who provided that advice, and whether any legal objections were raised during internal discussions, implicate the confidential internal deliberations of the Executive Branch. We are not able to address those issues.

6. **How many U.S. persons have had their calls or e-mails monitored or have been subjected to any type of surveillance under the NSA's warrantless electronic surveillance program?**

Operational details about the scope of the Terrorist Surveillance Program are classified and sensitive, and cannot be discussed in this setting. Openly 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.

7. **General Hayden has said that the NSA program does not involve data mining tools or other automated analysis of large volumes of domestic communications. Can you confirm that? Has the NSA program *ever* involved data mining or other automated analysis of large volumes of communications of any sort?**

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 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.

8. **Are there other programs that rely on data mining or other automated analysis of large volumes of communications that feed into or otherwise facilitate either the warrantless surveillance program or the FISA warrant process?**

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. 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 congressional leadership.

9. **Has the Justice Department issued any legal advice with regard to the legality or constitutionality of the NSA or other agencies in the Intelligence Community conducting data mining or other automated analysis of large volumes of domestic communications? If so, please provide copies.**

We cannot reveal confidential legal advice delivered within the Executive Branch or its internal deliberations. If legal advice from Executive Branch officers or entities were subject to disclosure, those who need legal advice would be reluctant to seek it, and those responsible for providing candid legal advice might be discouraged from giving it. That would increase the risk of legal errors. Nor can we discuss the existence (or non-existence) of any specific intelligence activities.

10. **What is the longest duration of a surveillance carried out without a court order under this warrantless electronic surveillance program? What is the average length?**

This question calls for classified and sensitive operational details of the Terrorist Surveillance Program that cannot be discussed here. Openly 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.

11. **Did we understand correctly from your testimony that the NSA is only authorized to intercept communications when a "probable cause" standard is satisfied, and that it is "the same standard" as the one used under FISA? Has that been true since the inception of this program?**

As we have said, the Terrorist Surveillance Program targets for interception 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. This "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("[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.

12. What standard for intercepting communications without a warrant was the NSA applying when the program was first authorized? What standard was the NSA applying in January 2004?

The Terrorist Surveillance Program targets communications for interception only 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. We can discuss only the Terrorist Surveillance Program. We cannot discuss the operational history or details of the Terrorist Surveillance Program or any other intelligence activities.

13. Did the standard change after there were objections from the FISA Court? Did the standard change after there were objections from senior Justice Department officials?

We cannot discuss the operational details or history of the Terrorist Surveillance Program. Nor can we divulge the internal deliberations of the Executive Branch or the content of our discussions with the Foreign Intelligence Surveillance Court.

14. Who decides whether the "probable cause" standard has been satisfied? Who if anyone reviews this decision? Are records kept as to the satisfaction of this condition for each surveillance?

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, these officers determine 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. Steps are taken to enable appropriate oversight of interception decisions.

15. Did we understand correctly from your testimony that, under this program, the NSA is authorized to intercept communications only when one party to the communication is outside the United States? Has that always been true? Describe the history and legal significance of that limitation.

The Terrorist Surveillance Program targets communications for interception only where one party is outside the United States. It does not target domestic communications—that is, communications that both originate and terminate within the United States. The targeting of international communications for interception fits comfortably within this Nation's traditions. Other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force authorizations such as the Force Resolution enacted by Congress to permit warrantless surveillance of international

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"). We are not able to discuss further the history or operational details of the Program.

16. **What does this limitation mean with respect to e-mail communications? Must either the person sending the e-mail or one of persons to whom the e-mail is addressed be physically located outside the United States? Has that always been true?**

As the President has stated, the Terrorist Surveillance Program targets for interception communications only where one party is outside the United States. We cannot openly reveal operational details about how the NSA determines that a communication meets that standard, which could compromise the Program's value by facilitating terrorists' attempts to evade it.

17. **Who decides whether one party to a communication is outside the United States? Who if anyone reviews this decision? Are records kept as to the satisfaction of this condition for each surveillance?**

Professional intelligence officers at the NSA determine whether an international communication meets the standards of the Terrorist Surveillance Program—that is, that there is probable cause to believe that at least one party is a member of al Qaeda or an affiliated terrorist organization. Appropriate records are kept and procedures are in place to ensure that decisions can be reviewed by the NSA Office of General Counsel and the NSA Inspector General.

18. **Does FISA under any circumstances require the government to obtain a court order to target and wiretap an individual who is overseas? Does it make a difference whether that targeted person who is overseas calls someone in the United States?**

FISA defines "electronic surveillance" to include the acquisition of the contents of "any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2). Thus, if the procedures of FISA applied, and if the actual acquisition of a wire communication occurred in the United States, FISA would require a court order to intercept wire communications between a person in the United States and a person overseas. Likewise, the installation or use of a surveillance device inside the United States to acquire information could, under some circumstances, require a FISA order, regardless of the location of the target of the surveillance. *See* 50 U.S.C. § 1801(f)(4).

19. **Did we understand correctly from your testimony that under this program the NSA is authorized to intercept communications only when at least one party to the communication is "a member or agent of al Qaeda**

or an affiliate terrorist organization"? Has that always been true? Describe the history of that standard and if and how it has changed over time.

Under the Terrorist Surveillance Program, the NSA is authorized to target for interception communications where one party is outside the United States and 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. We cannot discuss operational details or history of the Terrorist Surveillance Program.

20. **Who decides whether at least one party to a communication is "a member or agent of al Qaeda or an affiliate terrorist organization"? Who decides whether an organization is "an affiliate terrorist organization"? Who if anyone reviews these decisions? Are records kept as to the satisfaction of these conditions for each surveillance?**

Professional intelligence officers at the NSA who are experts on al Qaeda and its tactics (including its use of communications systems) decide whether 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. Those decisions are subject to appropriate and rigorous oversight, and appropriate records are kept and procedures are in place to ensure that decisions are able to be reviewed by the NSA Office of General Counsel and the NSA Inspector General. There is also an extensive interagency review process as to what constitutes a terrorist organization affiliated with al Qaeda.

21. **Are the above standards and limitations (probable cause; one party is outside the United States; one party is al Qaeda or al Qaeda affiliate) contained in the President's authorizations? Has that been true since the inception of the program? If these limitations have not always been contained in the President's authorizations, how have they been communicated to the NSA?**

We cannot discuss the operational details or history of the Program or any other intelligence activities.

22. **What percentage of the communications intercepted pursuant to this program generate foreign intelligence information that is disseminated outside the NSA? How does that compare to the percentage of disseminable communications intercepted pursuant to FISA?**

As we have explained above and elsewhere, this type of operational information about the Terrorist Surveillance Program is classified and sensitive, and cannot be discussed here.

23. **Under your interpretation of FISA's Authorization During Time of War provision [50 U.S.C. § 1811], if Congress in September 2001 had not only**

authorized the use of "all necessary and appropriate force" against al Qaeda, but also formally declared war, would the 15-day limit on warrantless electronic surveillance have applied?

Section 111 of FISA, 50 U.S.C. § 1811, provides an exception from FISA procedures for a 15-day period following a congressional declaration of war. As discussed in the January 19th paper, FISA's legislative history makes clear that Congress provided this period to give Congress and the President an opportunity to produce legislation authorizing electronic surveillance during the war. And that is precisely what the Force Resolution does—it authorizes the use of electronic surveillance outside traditional FISA procedures.

There is no reason why section 109(a) of FISA, 50 U.S.C. §1809(a)—which contemplates that future statutes might authorize further electronic surveillance—could not be satisfied by legislation authorizing the use of force. In response to your question, we believe that both 50 U.S.C. § 1811 and the Force Resolution would authorize the Terrorist Surveillance Program during the 15-day period after a declaration of war, and that the Force Resolution would authorize the Program thereafter.

24. **Your analysis relies heavily on section 109(a)(1) of FISA, which provides criminal penalties for someone who intentionally "engages in electronic surveillance under color of law *except as authorized by statute*." According to the legislative history of this provision, the term "except as authorized by statute" referred specifically to FISA and the criminal wiretap provisions commonly known as "title III". The House Intelligence Committee report (p.96) states, "Section 109(a)(1) carries forward the criminal provisions of chapter 119 [title III] and makes it a criminal offense for officers or employees of the United States to intentionally engage in electronic surveillance under color of law *except as specifically authorized in chapter 119 of title III and this title*." Similarly, both the Senate Intelligence Committee report (p.68) and the Senate Judiciary Committee report (p.61) explain that section 109 was "designed to establish the same criminal penalties for violations of this chapter [FISA] as apply to violations of chapter 119 [title III]. ... [T]hese sections will make it a criminal offense to engage in electronic surveillance *except as otherwise specifically provided in chapters 119 [title III] and 120 [FISA]*." In interpreting what Congress intended by the term "except as authorized by statute," did the Justice Department know of the existence of this Committee Report language? If so, why did the Justice Department not feel compelled to discuss this clarifying language?**

The Department's January 19th paper discussed the most pertinent authorities bearing on the legality of the Terrorist Surveillance Program, such as the Constitution, the language of FISA, and the *Hamdi* decision. The legislative history you reference not only does not undermine the Department's conclusion, it supports it.

To begin with, those passages of legislative history cannot be taken at face value 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 use 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 could have been used to authorize the installation and use of pen registers, Chapter 119 of Title 18 could not. Thus, if the passages of legislative history cited in your question were to be taken at face value, 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 have been authorized outside the foreign intelligence context. Moreover, it is perfectly natural that the legislative history would mention only FISA and chapter 119, since they were the principal statutes in 1978 that authorized electronic surveillance as defined in FISA.

What this legislative history demonstrates is that Congress knew how to make section 1809(a)(1)'s reference to "statute" more limited if it had wished to do so. Indeed, it appears that Congress deliberately chose not to mimic the restrictive language of former 18 U.S.C. § 2511(1). By using the term "statute," Congress made clear that not only the existing authorizations for electronic surveillance in chapter 119 of title 18 and in title 50, but also those that might come in future statutes, would satisfy FISA. Congress was wise to include that flexibility, in light of the fact that it was legislating for the first time with respect to constitutional authority that the President previously had exercised alone.

25. **The Administration has argued that the NSA's activities do not violate the Fourth Amendment because they are reasonable. Are the intelligence officers who are deciding what calls to monitor the final arbiters of what is "reasonable" under the Fourth Amendment? Who makes the final determination as to what is constitutionally "reasonable"?**

The President has indicated that the Terrorist Surveillance Program is limited to targeting for interception 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 light of the paramount government interest in avoiding another catastrophic terrorist attack resulting in massive civilian deaths, this narrowly tailored program is clearly reasonable for purposes of the Fourth Amendment. That conclusion is underscored by the fact that the Terrorist Surveillance Program is subject to review every 45 days to determine whether it continues to be necessary. Intelligence officers are not making the determination of what is "reasonable" under the Fourth Amendment; instead, they make a factual determination that the "probable cause" standard is met in a particular instance. That is quite appropriate, as the courts have stressed that probable cause determinations are not technical, legal conclusions, but rather are conclusions based on the practical considerations of everyday life on which reasonable persons act.

26. You indicated that "career attorneys" at NSA and Justice approved the program. It has been reported that non-career attorneys at these agencies did not agree. Please identify those who you say approved the program, those who did not approve of it, and the nature of the disagreement.

This question asks for details about the internal deliberations of and the confidential legal advice delivered within the Executive Branch, and we are not in a position to provide such information.

27. How many people within the NSA, DOJ, the White House, or any other federal agency have been involved in the authorization, implementation, and review of the NSA program?

The President, Vice President, General Hayden, and the Attorney General have stated publicly that they were involved in the authorization, implementation, and/or review of the Terrorist Surveillance Program. We have also explained that the NSA Office of General Counsel and Office of Inspector General are involved in the oversight and review of the program, and that professional intelligence officers at the NSA are involved in the day-to-day implementation of the program. Lawyers at the Department of Justice and officials at the Office of the Director of National Intelligence are also involved in the review. We cannot provide further information, as it concerns internal deliberations of the Executive Branch and classified and sensitive information about the Program.

28. You have mentioned various people in the Intelligence Community who approved of these activities, including the NSA Inspector General. But you have not mentioned the person in that community statutorily assigned to review and assess all such programs -- the Civil Liberties Protection Officer for the Office of the Director of National Intelligence. Does your failure even to mention him mean that you were not aware of his role, that a decision was made not to inform him of the program, or that he was familiar with the program but did not approve of it?

It may provide some context for this question to note that the Director of National Intelligence was created by statute in December 2004, and the Director position was filled only in April 2005. The Civil Liberties Protection Officer was filled on an interim basis only in June 2005, and that interim appointment was made permanent in early December 2005. As stated above, we cannot reveal further details about who was cleared into this Program or the internal deliberations of the Executive Branch.

29. You have said that the NSA program is subject to internal safeguards and said it is reviewed approximately every 45 days. Who conducts those reviews? What are the questions they are asked to review and answer? Do they produce any written products? If so, please provide copies.

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," 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. While some of those procedures cannot be described in this setting, the oversight program includes review by lawyers at the National Security Agency 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. We cannot disclose documents generated by these reviews, which involve the internal deliberations and confidential legal advice of the Executive Branch and classified and sensitive information.

30. Do the 45-day reviews include any determination of the effectiveness of the program and whether it has yielded results sufficiently useful to justify the intrusions on privacy? If so, are such determinations based on quantitative assessments of third parties or subjective impressions of the people involved in the surveillance activities?

As noted above, the 45-day review does account for the effectiveness of the Terrorist Surveillance Program and considers privacy interests.

31. As part of this program, have any certifications been provided to telecommunications companies and Internet Service Providers that "no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required," as set out in 18 U.S.C. § 2511(2)(a)(ii)? If yes, how many were issued and to which companies?

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.

32. Can information obtained through this warrantless surveillance program legally be used to obtain a warrant from the FISA Court or any court for wiretapping or other surveillance authority? Can it legally be used as evidence in a criminal case? Has it been used in any of these ways? Has the FISA court or any court ever declined to consider information obtained from this program and if so, why?

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.

33. Are you aware of any other Presidents having authorized warrantless wiretaps outside of FISA since 1978 when FISA was passed?

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. During the hearing, you have repeatedly qualified your testimony as limited to, *e.g.*, "those facts the President has publicly confirmed," "the kind of electronic surveillance which I am discussing here today," "the program I am talking about," "the program which I am testifying about today," "the program that we are talking about today," "the program that I am here testifying about today," and "the terrorist surveillance program about which I am testifying today." Please explain what you meant by these qualifications. Aside from the program that you testified about on February 6, 2006, has the President secretly authorized any additional expansions or modifications of government surveillance authorities with respect to U.S. persons since September 11, 2001? If so, please describe them and the legal basis for their authorization.

The decision to reveal classified information about the Terrorist Surveillance Program rests with the President. *See Department of the Navy v. Egan*, 484 U.S. 518, 530 (1988). The quoted statements reflect the fact that the Attorney General was authorized to discuss only the Terrorist Surveillance Program and the legal authorities supporting the Program. He was not authorized to discuss any operational details of the

Program or any other intelligence activity of the United States in an open hearing, though our inability to respond should not be taken to suggest that there are such activities.

35. Has the President taken or authorized any other actions that would violate a statutory prohibition and therefore be illegal if not, under your view of the law, otherwise permitted by his constitutional powers or the Authorization for Use of Military Force? If so, please list and describe those actions, and provide a chronology for each.

Five members of the Supreme Court concluded in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), that the Force Resolution satisfies 18 U.S.C. § 4001(a)'s prohibition on detention of U.S. citizens "except pursuant to an Act of Congress," and thereby authorizes the detention of Americans who are enemy combatants. FISA contains a similar provision indicating that it contemplates that warrantless electronic surveillance could be authorized in the future "by statute." Specifically, section 109 of FISA prohibits persons from "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*." 50 U.S.C. § 1809(a)(1) (emphasis added). Just as the Force Resolution satisfies the statutory authorization requirement of 18 U.S.C. § 4001(a), it also satisfies the comparable requirement of section 109 of FISA.

We have not sought to catalog every instance in which the Force Resolution or the Constitution might satisfy a statutory prohibition contained in another statute, other than FISA and section 4001(a), the provision at issue in *Hamdi*. We have not found it necessary to determine the full effect of the Force Resolution to conclude that it authorizes the Terrorist Surveillance Program.

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.