U.S. Department of Justice

National Security Division

Washington, D.C. 20530

FEB 18

NSD FOI/PA #09-007

Mr. Steven Aftergood
Senior Research Analyst
Federation of American Scientists
1725 DeSales Street, N.W., 6th Floor
Washington, D.C. 20036

Dear Mr. Aftergood:

This is in response to your August 25, 2008, Freedom of Information Act request for a copy of Assistant Attorney General Kenneth Wainstein's written answers to questions before the House Judiciary Committee on September 18, 2007.

A copy of this item is enclosed.

Sincerely,

Arnetta James
FOIA Coordinator
Office of Law and Policy

Enclosure

Doc. Ref. in Jan

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 15, 2009

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of then-Assistant Attorney General Kenneth Wainstein before the Committee on September 18, 2007, at a hearing entitled "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)." We apologize for the time necessary to prepare these responses. We hope that this information is of assistance to the Committee. Please do not hesitate to call upon us if we may be of additional assistance.

The Office of Management and Budget advises us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Keith B. Nelson
Principal Deputy Assistant Attorney General

Enclosure

cc: The Honorable Lamar S. Smith
Ranking Minority Member

Committee on the Judiciary
House of Representatives

"Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)"

September 18, 2007

Responses of the
Department of Justice
to Questions Posed to
Then-Assistant Attorney General
Kenneth L. Wainstein

Questions from September 11, 2007 Letter to White House Counsel Fred Fielding (Wainstein and McConnell)

1. **The Committee sent a September 11, 2007 letter to White House Counsel Fred Fielding containing a list of questions concerning Administration foreign intelligence surveillance activities, which can be found on pages 4-5 of the attached letter. To date, we have yet to receive answers to these questions, which the White House has indicated should come from the relevant agencies. Please respond to those questions as soon as possible.**

   Your questions generally relate to the highly classified details of particular intelligence activities allegedly conducted by the Government after September 11, 2001. The FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, resulted from extensive exchanges of information, briefings, and consultations between Congress and the Executive Branch. In order to better inform the debate concerning liability protection, the House Intelligence and Judiciary Committees were provided with access to documents and other information relating to the President's Terrorist Surveillance Program. It is the Department's understanding that these materials provided information sought with respect to the questions posed in the September 11, 2007 letter.

2. **Under the PAA, the FISA Court only has the ability to determine whether the government is following its own procedures, and can stop the procedures only if they are "clearly erroneous." How can meaningful oversight occur if the court can only review procedures that it did not even initially approve under a "clearly erroneous" standard, rather than the underlying legality of the government's surveillance operations? Please explain.**

The "clearly erroneous" standard of review is one that appeared in FISA prior to the PAA, 50 U.S.C. §§ 1805(a)(4); 1824(a)(4), and is an appropriate level of review for the foreign intelligence activities authorized under the Protect America Act—those targeting terrorists and other national security threats abroad. Under section 105B, the Director of National Intelligence and the Attorney General could have authorized, subject to certain limitations, the acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States. 50 U.S.C. § 1805B (since repealed). The court would then have reviewed the determination of the Director of National Intelligence and the Attorney General that the required procedures were reasonably designed to determine that such acquisitions concerned persons reasonably believed to be located outside the United States. 50 U.S.C. § 1805C (since repealed). Given that the Act was focused on intelligence activities directed at persons located outside the United States, the "clearly erroneous" standard of review was appropriate and a higher standard of review would not have increased significantly the protection of the privacy interests of Americans. Moreover, this standard of review permitted the court to exercise substantial oversight powers, including ordering the Government to submit new procedures or cease an acquisition, if the court found the Government's determination to be clearly erroneous. 50 U.S.C. § 1805C(c) (since repealed).

In addition, the Government applied the statute in the full view of congressional oversight. We provided Congress with consistent and comprehensive insight into our implementation and use of this authority. As we publicly committed, we informed the full membership of the Intelligence and Judiciary Committees concerning the implementation of this new authority and the results of the reviews that the Department of Justice and the Office of the Director of National Intelligence conducted to assess and ensure compliance by the implementing agencies; we provided those Committees with copies of the written reports of those compliance reviews; and we made ourselves available to brief members and staffs about compliance and implementation on a monthly basis. In fact, representatives of the Executive Branch provided several detailed briefings to Members and staff on the implementation of the Protect America Act. These included on-site briefings for staff members by agencies implementing the Act. In addition, we provided the committees with copies of documents related to our implementation of this authority, including the relevant certifications and procedures required by the statute (with redactions as necessary to protect critical intelligence sources and methods).

Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain the approval of the Foreign Intelligence Surveillance Court (FISC) of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a. The FISC reviews these procedures de novo.

4. **Is it correct that the "minimization" procedures that are to apply to surveillance under PAA are those specified under 50 U.S.C. sec. 1801(h)(1)-(3)? If not, which procedures apply?**

The Protect America Act required the Director of National Intelligence and the Attorney General to certify that the minimization procedures to be used with respect to acquisitions under section 105B met the definition of minimization procedures under 50 U.S.C. § 1801(h). Since section 1801(h)(4) applies to "electronic surveillance approved pursuant to section 1802(a)," the minimization procedures used for acquisitions under section 105B were required to meet the definition of minimization procedures in 50 U.S.C. § 1801(h)(1)-(3).

As amended, FISA contains a similar requirement. *See* 50 U.S.C. § 1881a.

8. **Does section 105(B) permit the President to compel communications carriers to conduct domestic wiretaps so long as "a significant purpose" is to obtain foreign intelligence information concerning persons outside the United States?**

We understand your reference to "domestic wiretaps" to refer to the interception of purely domestic communications (*i.e.*, communications between two persons in the United States). Such activities could not have been conducted under the authorities provided by section 105B. That section required the Director of National Intelligence and the Attorney General to certify for any acquisition under that section that the "acquisition does not constitute electronic surveillance." 50 U.S.C. § 1805B(a)(2) (since repealed). The PAA did not change the definition of "electronic surveillance" under FISA with respect to the acquisition of purely domestic communications. Therefore, the PAA did not alter the FISA requirement to obtain a court order for the interception of purely domestic communications.

9. **If an individual in the United States is suspected of working in collusion with persons outside the United States—such that an investigation of one is in effect the investigation of the other—under what circumstances, generally, would you use criminal or other FISA wiretaps, and under what circumstances would you use 105(B) authority? Please explain.**

While the Protect America Act provided that nothing in FISA's definition of "electronic surveillance" "shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States," 50 U.S.C. § 1805A (since repealed), it did not change FISA's underlying definition of "electronic surveillance" with respect to persons in the United States. Thus, even following the passage of the

Protect America Act, surveillance targeting a person in the United States that constituted "electronic surveillance" under FISA continued to be governed by FISA's requirements and, as a result, the Protect America Act could not have been used to target persons inside the United States.

10. **Assuming for a moment that a member of Congress is going to meet with a high-ranking official from Syria, does Section 105(B) permit the wiretapping of that Member's office phone on the grounds that it would produce "foreign intelligence information . . . concerning persons reasonably believed to be outside the United States?" Please explain.**

No. Section 105B required the Director of National Intelligence and the Attorney General to certify for any acquisition under that section that the "acquisition does not constitute electronic surveillance." 50 U.S.C. § 1805B(a)(2) (since repealed). The activity you describe—targeting a Member of Congress inside the United States—would remain "electronic surveillance" under FISA, because it meets the first definition of "electronic surveillance" under that statute. *See id.* § 1801(f)(1). That definition includes "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." *Id.* Since the activity would be electronic surveillance, the pre-Protect America Act court order requirements of FISA would apply, and the Government could not conduct such surveillance pursuant to a certification issued under section 105B.

Furthermore, the FISA Amendments Act of 2008, passed by a bipartisan majority in both Houses of Congress and signed by the President, appropriately addresses concerns, like those in the question, raised about the PAA.

11. **Does Section 105(B) permit searching stored emails of a Member of Congress who is planning to meet with Iraqi officials? Please explain.**

Section 105B required any acquisition conducted under the Protect America Act to have been "concerning persons reasonably believed to be outside the United States." 50 U.S.C. § 1805B(a) (since repealed). We did not interpret that phrase to include acquisitions targeting a person in the United States who is communicating with someone outside the United States. Thus, even if the purpose of the acquisition was to acquire information concerning foreign officials outside the United States, we could not have used the Protect America Act to target a Member of Congress or any other person in the United States to do so. Moreover, any collection effort contemplating the targeting of a

Member of Congress would, of course, raise additional and significant legal and prudential considerations.

12. **Assuming for a moment that an official at a West Coast computer company is negotiating with China to sell certain computer technology—that may or may not be sensitive, the facts are simply not certain—does Section 105(B) permit the searching of the executive's emails on the grounds that all information associated with the transaction is "foreign intelligence information . . . concerning persons reasonably believed to be outside the United States"? Please explain.**

Please see the response to Question 11.

13. **Under Section 105(B) does the term "acquire" include "intercept"? Can the Administration "acquire" foreign relations information concerning persons overseas by "intercepting" phone conversations in the United States? Please explain.**

The answer to your first question is yes. Section 105B required the Director of National Intelligence and the Attorney General to certify, among other things, that the acquisition of foreign intelligence information would have been "from or with the assistance of a communications service provider, custodian, or other person . . . who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." 50 U.S.C. § 1805B(a)(3) (since repealed). The PAA did not specify the manner in which the Government could complete an acquisition, so foreign intelligence information could have been acquired through various techniques, including the interception of communications.

With respect to your second question, if the activity you describe were targeting a person overseas, such collection could have occurred under the Protect America Act. If the activity you describe were electronic surveillance targeting a person in the United States, however, such surveillance would be governed by FISA. Section 105B required the Director of National Intelligence and the Attorney General to certify that the "acquisition does not constitute electronic surveillance." 50 U.S.C. § 1805B(a)(2) (since repealed). "Electronic surveillance" is defined in 50 U.S.C. § 1801(f) as:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a

person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

While the Protect America Act provided that nothing in that definition "shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States," 50 U.S.C. § 1805A (since repealed), the definition of "electronic surveillance" was unchanged with respect to persons in the United States.

14. Under Section 105(B) does the term "custodian" refer to anyone other than "custodians" of communications carriers?

No. We believe the language of section 105B(a)(3) authorized acquisitions only from or with the assistance of entities that provide communications services. Section 105B only allowed the Attorney General and the Director of National Intelligence to authorize those activities that, among other limitations, involved obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." 50 U.S.C. § 1805B(a)(3) (since repealed). In applying this provision of the Protect America Act,

which has since been repealed, we interpreted the term "custodian" to apply only to custodians of a communications service provider.

In addition, the FISA Amendments Act of 2008, passed by a bipartisan majority in both Houses of Congress and signed by the President, appropriately addresses concerns, like those in the question, raised about the PAA. In particular, as amended, FISA requires that the Attorney General and Director of National Intelligence certify that acquisition "involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider." *See* 50 U.S.C. § 1881a. The term electronic communication service provider is defined in section 701 of FISA, as added by the FISA Amendments Act of 2008, and does not include the term custodian. *See* 50 U.S.C. § 1881(b)(4).

a) **Can the President direct a "custodian" of a medical office to turn over medical records, if a "primary purpose" of the investigation is to obtain foreign intelligence information concerning someone who is overseas? Please explain.**

Please see the answer to question 14 above.

b) **Can the President direct a "custodian" of a business, bank, or credit agency to turn over financial records to the Government, so long as a "significant purpose" of the request is to obtain foreign intelligence information? Please explain.**

Please see the answer to 14 above.

15. **Suppose an American critic of the Iraq War travels overseas, and is thus no longer in the United States. Under Section 105(B), can the President direct "custodians" of records concerning this individual, including stored electronic communications, to produce records to the Government with no other showing of cause that is subject to judicial review? Please explain.**

Please see the answer to 14 above. In addition, under section 702 of FISA, as added by the FAA, the government may not intentionally target a United States person reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b)(3).

16. **18 U.S.C. § 2511(2)(a)(ii) currently provides for telecommunications carrier immunity if one of two conditions is satisfied: a) the carrier has a court order signed by an authorizing judge; or b) the carrier has a certification from the Attorney General or another statutorily authorized official that no warrant or court order is required by law, that all statutory requirements have been met, and that the**

specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance required. Doesn't this current statutory scheme offer the necessary protection for the telecommunications industry, advance national security interests, and provide essential oversight? If not, why not?

The FISA Amendments Act provides liability protection to companies that either did not act or received either court orders, statutory certifications under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, certain statutory directives, or certain written requests or directives from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) indicating that the activity was authorized by the President and determined to be lawful. *See* 50 U.S.C. § 1885a(a). We believe this provides appropriate liability protection for prospective activities as well as for a limited group of telecommunications providers who, as the Senate Intelligence Committee found, acted in good faith in assisting the Government with a discrete set of intelligence activities in the aftermath of September 11, 2001.

17. **Section 2511(2)(a)(ii) certification has defined preconditions that must be satisfied, including: all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Blanket immunity would not have the same preconditions. Given that distinction, how can we ensure that critical checks and balances exist in the surveillance framework if blanket immunity is provided?**

The FISA Amendments Act does not provide blanket immunity. Rather, it requires dismissal of a lawsuit only if one of five limited circumstances is met: (1) the alleged assistance was provided pursuant to court order; (2) the alleged assistance was provided pursuant to a certification under section 2511(2)(a)(ii)(B) or 2709(b) of title 18; (3) the alleged assistance was provided pursuant to certain statutory directives specified in FISA, the Protect America Act, and the FISA Amendments Act; (4) the alleged assistance was (a) provided in connection with a communications intelligence activity that was (i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, and (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States, and (b) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was (i) authorized by the President, and (ii) determined to be lawful; or (5) the alleged assistance was not provided. 50 U.S.C. § 1885a(a). The certification is to be

given effect unless the court finds that it is not supported by substantial evidence provided pursuant to the Act. 50 U.S.C. § 1885a(b). The Act does not immunize criminal conduct or conduct of the Government. *See* 50 U.S.C. § 1885a.

18. **If we were to give the telecommunications carriers complete, blanket immunity, how would we guard against a total disregard of the law by companies who believe that the government simply will bail them out if they overstep legal boundaries in intercepting communications?**

As explained above, the FISA Amendments Act does not provide for blanket immunity, but rather is limited in scope and protects only those companies that either did not provide the alleged assistance, or acted pursuant to a court order, statutory directive or certification, or a written directive or request from a high ranking government official indicating that the activity was authorized by the President and determined to be lawful. *See* 50 U.S.C. § 1885a(a).

As for particular intelligence activities examined by the Senate Intelligence Committee, the Committee concluded that the providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. S. Rep. No. 110-209 at 10. Because the committee "concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received," *id.* at 11, the committee concluded that the providers "should be entitled to protection from civil suit." *Id.* The provision is a one-time grant of retroactive immunity for a discrete set of activities designed to "detect and prevent the next terrorist attack" after September 11th. *Id.* As the Intelligence Committee stated, the immunity "should be understood by the Executive branch and providers as a one-time response to an unparalleled national experience in the midst of which representations were made that assistance to the Government was authorized and lawful." *Id.* at 12.

We also believe that existing congressional oversight mechanisms are sufficient to help keep Congress informed of intelligence activities.

19. **If the so-called Terrorist Surveillance Program (TSP) was perfectly legal as has been claimed, why would companies who cooperated in it need immunity?**

There are many factors that supported the enactment of liability protection apart from the legality of the NSA activities acknowledged by the President that subsequently have been referred to as the Terrorist Surveillance Program ("TSP"). Companies have been subject to lawsuits to determine the precise facts concerning alleged intelligence activities, and such suits risk the disclosure of classified information that could compromise ongoing intelligence activities, sources, and methods. Such suits also can be lengthy, costly, and

unpredictable, thereby deterring private individuals and entities from helping the Government in vital counterterrorism efforts in the future. As noted in response to question 18, above, the Senate Intelligence Committee concluded that retroactive immunity was a necessity.

In addition, the lawsuits at issue allege that particular companies were involved in activities beyond those publicly described by the President. Any inquiry in litigation into any alleged role particular companies played in the TSP or into other alleged activities would require the disclosure of classified facts concerning intelligence sources and methods, such as whether or not certain alleged activities even existed and specifically how any such alleged activities would have been conducted. The disclosure of such information would severely harm U.S. national security by helping our adversaries evade detection. Additionally, the prevention of such disclosures is important to the security of the facilities and personnel of relevant electronic communication service providers.

23. **Section 105(A) exempts surveillance "directed at" people overseas from the definition of electronic surveillance, and therefore traditional FISA court review. Because surveillance only need be "directed" at people overseas, can the government under the PAA pick up all international communications into or out of the U.S., as long as one party to the call is overseas?**

The FISA Amendments Act of 2008, enacted on July 10, 2008, did not contain a carve-out of the definition of electronic surveillance analogous to that contained in the PAA. In addition, it is important to note that if the target of intelligence collection is a person in the United States, FISA requires the Government to go to the Foreign Intelligence Surveillance Court for an order to conduct electronic surveillance of that target — under the same circumstances it would have before the Protect America Act passed. In the same way, section 702 of FISA, as added by the FISA Amendments Act of 2008, provides that the authority granted by that section, to target persons reasonably believed to be located outside the United States to obtain foreign intelligence, cannot be used to intentionally target any person known at the time of the acquisition to be located in the United States, nor can it be used to intentionally target a person reasonably believed to be outside the United States if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States. 50 U.S.C. § 1881a.

24. **FISA has always placed the telecommunication carriers between the government and American's private communications and records. The carriers can only turn over information in response to a specific request. Now that the government has direct access to all communication streams, how can we protect against potential abuses?**

The Protect America Act did not give the Government "direct access to all communication streams." Section 105B allowed the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." 50 U.S.C. § 1805B(a)(3) (since repealed). Therefore, telecommunications carriers remained integral to such activities under section 105B. In addition, section 105B included a provision under which an entity or person, such as a telecommunications carrier, receiving a directive from the Attorney General can challenge the legality of that directive in the FISC. *Id.* § 1805B(h) (since repealed).

The FISA Amendments Act of 2008 similarly requires that acquisitions under section 702 of FISA, as added by the FISA Amendments Act of 2008, "involve[] obtaining foreign intelligence information from or with the assistance of an electronic communication service provider." *See* 50 U.S.C. § 1881a. The term electronic communication service provider is defined in section 701 of FISA, as added by the FISA Amendments Act of 2008. In addition, the FAA contains extensive executive, judicial, and congressional oversight provisions, including a requirement that the AG and the DNI conduct semiannual assessments of compliance with targeting and minimization procedures and submit those assessments to the FISC and to Congress; that the FISC and Congress also receive annual reviews relating to those acquisitions prepared by the heads of agencies that use the authorities of the Act; that Congress receive reviews from the Inspector General of these agencies and the Department of Justice regarding compliance under the Act; that the AG submit to Congress a report at least semiannually concerning the implementation of the authorities provided by the Act and an expanded category of FISA-related court documents that the Government must provide to the congressional intelligence and judiciary committees.

26. **On May 11, 2006, USA Today reported that "[t]he NSA has been secretly collecting the phone call records of tens of millions of Americans" and that "[i]t's the largest database ever assembled in the world." (*See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls, USA Today*, May 11, 2006). At any time from September 11, 2001 to the present, has the Administration, pursuant to foreign intelligence purposes, obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of the specific title of the intelligence program or the agencies that conducted the program? Please explain.**

In keeping with longstanding practice, we can neither confirm nor deny in this setting any asserted intelligence activities or any aspects of such activities referred to in your question. Our inability to discuss such asserted programs in this setting should not be taken as an indication that any such programs exist. As a general matter, however, consistent with the reporting requirements of the National Security Act and long-standing practice, the Executive Branch notifies Congress of the classified intelligence activities of the United States through appropriate briefings.

FISA Exclusivity (Wainstein only; Answers provided by Department of Justice)

27. **Does the United States, through its Justice Department, agree that FISA is the law of the land, and that foreign intelligence surveillance must occur within that law? If not, why not?**

Foreign intelligence surveillance must be conducted in accordance with the Constitution and laws of the United States. A duly enacted statute, FISA has been and continues to serve as the framework for conducting "electronic surveillance," a term carefully defined by FISA, of foreign powers and agents of foreign powers. The Protect America Act of 2007 ("PAA") avoided potential conflicts between pre-PAA FISA and the well-recognized core executive branch function of protecting the United States from foreign threats, because it provides a statutory mechanism for conducting critical foreign intelligence surveillance activities. The FISA Amendments Act of 2008 continues to provide this statutory authority.

28. **Is the President free to disregard any provisions of FISA with which he disagrees? If so, please explain.**

The President is constitutionally obligated to "take Care that the Laws be faithfully executed," of which FISA is one. Thus, the President is not free to disregard any provision of FISA with which he simply disagrees nor is he free to disregard the Constitution, which he is also obligated to preserve, protect, and defend. Congressional attempts to circumscribe the President's power to conduct foreign intelligence surveillance in order to carry out his core constitutional duty to protect the nation raise difficult constitutional questions. The Protect America Act of 2007 avoided any potential conflict between FISA and the core Executive Branch function of protecting the United States from foreign threats because it provided a statutory mechanism for conducting critical foreign intelligence surveillance activities. The FISA Amendments Act of 2008 continues to provide this statutory authority.

29. **To your knowledge, since January of 2007, when the Attorney General stated that the TSP was brought within FISA, has all foreign intelligence electronic surveillance occurred consistent with FISA — both prior to and subsequent to the August**

amendments? Since that time have any electronic surveillance programs been conducted outside the authority of the Foreign Intelligence Surveillance Act as amended by the Protect America Act?

Since January 2007, electronic surveillance for foreign intelligence purposes has been done pursuant to orders and authorizations under the Foreign Intelligence Surveillance Act, including as it was amended by the Protect America Act and the FISA Amendments Act of 2008.

30. **Does the Department of Justice still take the position that the Authorization for Use of Military Force (AUMF) related to the invasion of Iraq presently constitutes a basis for the President to disregard FISA? If so, please explain.**

As stated in response to Question 27, FISA has been and continues to serve as the framework for conducting electronic surveillance for foreign intelligence purposes. Section 109(a)(1) of FISA, 50 U.S.C. § 1809(a)(1), contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending or referencing FISA. The Department of Justice has articulated the position that the Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 ("Force Resolution"), passed by Congress on September 18, 2001, provides another congressional source of electronic surveillance authority (specific to the armed conflict with al Qaeda and its affiliated terrorist organizations). *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 2-3, 23-28 (Jan. 19, 2006). That remains the position of the Department of Justice.

This analysis did not rely on the Authorization for the Use of Military Force related to the Iraq conflict.

31. **On December 22, 2005, the Department of Justice, in a letter to Congress, set forth the position that the President's inherent Article II powers permitted it to conduct certain terrorist surveillance outside of FISA. Is this still the Department of Justice's position?**

The position articulated in the December 22, 2005 letter remains the position of the Department of Justice.

The Federal Bureau of Investigation (Wainstein only; Answers provided by Department of Justice)

32. **DNI McConnell said the intelligence community is not doing massive data mining. But the FBI retains information from NSLs even where the information**

demonstrates the subject of the NSL was innocent. Why is this data being retained if not for data mining?

The FBI has legitimate investigative reasons for retaining information properly collected during the course of authorized investigations, even if the data pertains to individuals who are initially determined not relevant to the investigation (for example, the target called a telephone number ten times, but the contact is determined to be innocuous).

The FBI retains such information for at least two investigative reasons. First, by retaining the records that form the basis for our determination that a person is not of investigative interest, the FBI is able to ensure that an audit trail exists so that the FBI does not re-investigate the person each time he or she appears in an investigation. Instead, FBI agents and analysts can simply revisit the information previously collected and satisfy themselves that the judgment previously made, that the person is not of concern to the FBI, is still valid. That can generally be done without intruding again on the person's privacy and without again collecting personal information about the individual. In contrast, if the FBI were to destroy the data, it would have to re-investigate the person each time he or she became pertinent to an investigation.

The second reason to retain information is equally important: in order to fulfill the Department's mission of keeping the country safe, we have been exhorted by Congress, the 9/11 Commission, the WMD Commission, and the American public to "connect the dots." The reality of analysis and investigative work is that connections between people that may seem entirely innocuous today can seem anything but innocuous when additional information is obtained. For that reason, the FBI needs to retain data and analysis regarding individuals so that, should the factual background change, the FBI still has the lawfully obtained information regarding those individuals. In short, using the jargon that has become prevalent, the FBI cannot "connect the dots" if it does not maintain the "dots" to connect.

33. **The Department of Justice Inspector General recently released an audit report regarding the Terrorist Screening Center, which revealed the Terrorist Screening Center watchlist had grown to over 724,000 records by April of 2007, and was increasing at a rate of 20,000 records per month. The IG found several known or suspected terrorists that were not watchlisted correctly, and a sample of records subjected to post-encounter quality - assurance reviews showed 38 percent contained errors or inconsistencies. How can the intelligence community properly identify and target terrorists for electronic surveillance with such an incomplete terrorist watchlist?**

The Terrorist Screening Database (TSDB) is not used to identify and target known or suspected terrorists for electronic surveillance. Known or suspected terrorists are watch

listed because they are already of interest to members of the Intelligence Community. Any decisions concerning targets for surveillance are made by law enforcement and intelligence agencies based on information in agency case management and intelligence systems. The TSDB's primary role is to support terrorism screening by agencies that have the authority to arrest, detain, or prevent known and suspected terrorists from entering the United States, or to identify those who may be in the United States during a law enforcement stop or seeking to gain access to areas of our Nation's critical infrastructure, such as airports. The TSDB is also extremely valuable to agencies charged with investigating or gathering intelligence on known and suspected terrorists. TSC, in coordination with the FBI's Terrorist Screening Operations Unit, relays information about encounters with persons in the TSDB to law enforcement and intelligence agencies for appropriate follow-up and for tactical and strategic analysis of the current terrorist threat.

Further, the Terrorist Screening Center (TSC) has taken multiple steps to enhance the data integrity of the TSDB. The TSC is currently involved in a comprehensive scrub of the entire TSDB to ensure it is accurate and up to date. The on-going scrub is similar to the scrub the TSC performed on the "No-Fly" portion of the TSDB, which resulted in the "No-Fly" records being reduced from approximately 65,000 to 31,592. Further, the TSC has brought on a full-time data integrity advisor to improve the quality and integrity of all data systems to include the TSDB, and made considerable progress in eliminating technical problems which caused some of the inconsistencies noted in the IG report. TSC has also augmented the nomination and redress processes to further improve the TSDB's data quality. The TSC appreciates the in-depth analysis by the OIG, and views the OIG's report as essential external scrutiny which provides an opportunity to improve the TSDB and make it an even more effective tool in the war on terrorism.