



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

APR 21 2008

Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA. 94110

Re: FOIA #08-060

Dear Ms. Hofmann:

This is our final response to your Freedom of Information Act (FOIA) request seeking access to "all agency records from September 1, 2007 to the present concerning briefings, discussions, or other exchanges that Justice Department officials have had with 1) members of the Senate or House of Representatives and 2) representatives or agents of telecommunications companies concerning amendments to FISA, including any discussion of immunizing telecommunications companies or holding them otherwise unaccountable for their role in government surveillance activities."

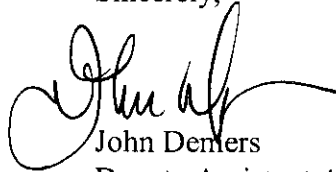
In response to your request, this Office released six documents in full, (totaling 24 pages) on April 8, 2008, and we have completed our review of the remaining records. Sixteen documents, (totaling 95 pages) are being released to you in full. Portions of two documents, (totaling 62 pages) are being released to you with excisions pursuant to Exemptions 1 and 3, 5 U.S.C. §552 (b)(1), and (b)(3), and one document is being withheld in full pursuant to the deliberative process privilege embodied in Exemption 5, 5 U.S.C. §552 (b)(5). Exemption 1 pertains to national security information which is properly classified pursuant to Executive Order 12958, as amended. Specifically, the withheld information is classified at the secret and top secret levels, which means that its unauthorized disclosure could reasonably be expected to cause serious and in some instances exceptionally grave damage to the national security of the United States. Exemption 3 permits the withholding of information specifically exempted from disclosure by statute. The applicable statute is the National Security Act of 1947, as amended, 50 U.S.C. § 403-1(1), which protects sensitive intelligence sources and methods. None of the information being withheld is appropriate for discretionary disclosure.

Twelve documents, totaling 57 pages were referred to the Office of the Director of National Intelligence and/or the Office of Information and Privacy, DOJ for review and direct response to you.

Finally, in response to your request, the Office of Information & Privacy referred six documents to this office for review and direct response to you. We have reviewed this material which consists of five *Statements* and *Written Testimony* by the Assistant Attorney General for National Security before Congress and a duplicate of NSD document #11. All of this material is appropriate for release without excision, and has been enclosed. For your convenience, we have also enclosed the remaining *Statements* and *Written Testimony* referenced in our April 8th correspondence to you.

Although your access request is the subject of litigation, you may administratively appeal this determination by writing to the Director, Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, NW, Suite 11050, Washington, D.C. 20530-0001, within sixty days from the date of this letter. Both the letter and envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

A handwritten signature in black ink, appearing to read "John Demers", with a stylized flourish extending to the right.

John Demers
Deputy Assistant Attorney General
Law and Policy

Enclosures: (24) documents
Document Index

EFF (HOFMANN) FOIA LITIGATION (FISA AMENDMENTS)
DISPOSITION OF NSD DOCUMENTS

<u>DOCUMENT #</u>	<u>DISPOSITION</u>
1	Released in full 4/21/08
2	Released in full 4/21/08
3	Referred to OIP/ODNI for direct response
4	Referred to OIP/ODNI for direct response
5	Referred to OIP/ODNI for direct response
6	Referred to ODNI for direct response
7	Referred to OIP/ODNI for direct response
8	Released in full 4/21/08
9	Released in full 4/8/08
10	Referred to ODNI for direct response
11	Released in full 4/21/08
12	Released in part 4/21/08
13	Released in part 4/21/08
14	Referred to OIP for direct response
15	Referred to OIP for direct response
16	Referred to OIP/ODNI for direct response
17	Released in full 4/21/08
18	Released in full 4/21/08
19	Referred to OIP for direct response
20	Released in full 4/21/08
21	Referred to ODNI for direct response
22	Released in full 4/21/08
23	Released in full 4/8/08
24	Released in full 4/21/08
25	Referred to OIP for direct response
26	Released in full 4/8/08
27	Released in full 4/8/08
28	Released in full 4/21/08
29	Released in full 4/8/08
30	Released in full 4/8/08
31	Withheld in full 4/21/08
32	Released in full 4/21/08
33	Released in full 4/21/08
34	Released in full 4/21/08
35	Released in full 4/21/08
36	Released in full 4/21/08
37	Released in full 4/21/08



U.S. Department of Justice

Office of Legislative Affairs

RELEASE

Office of the Assistant Attorney General

Washington, D.C. 20530

November 20, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of Mr. Kenneth Wainstein, Assistant Attorney General, National Security Division, for the hearing held before the Committee on October 31, 2007, entitled, "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

If we may be of further assistance, please feel free to contact this office.

Sincerely,

For Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosure

NSD-1



RELEASE

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 24, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

We understand that the Committee is holding a hearing tomorrow entitled, "Strengthening FISA-Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?" and that the Director of National Intelligence, J.M. McConnell, is scheduled to testify. We further understand that Director McConnell wrote to you suggesting that Assistant Attorney General Kenneth L. Wainstein appear as a co-witness with the Director.

The Department respects your prerogative as Chairman to structure Committee hearings in the manner that best addresses the Committee's need for information on critical issues like FISA modernization. Should you wish to hear from Mr. Wainstein at the hearing tomorrow, he stands ready and willing to testify. Moreover, we will remain ready to designate an appropriate witness to testify in the future if the Committee is interested in hearing from the Department of Justice on this critical legislation.

We appreciate the Committee's interest in this very important issue. Please do not hesitate to contact this office if we may be of assistance with this or any other matter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

cc: The Honorable Arlen Specter
Ranking Minority Member



JOHN CONYERS, JR., Michigan
 CHAIRMAN

WARD L. BERMAN, California
 BOUCHER, Virginia
 JERROLD NADLER, New York
 ROBERT C. "BOBBY" SCOTT, Virginia
 MELVIN L. WATT, North Carolina
 ZOE LOFORD, California
 SHEILA JACKSON LEE, Texas
 MAXINE WATERS, California
 WILLIAM D. DELAHUNT, Massachusetts
 ROBERT WIDLER, Florida
 LYDIA T. SANCHEZ, California
 STEVE COHEN, Tennessee
 HENRY C. "HANK" JOHNSON, JR., Georgia
 BETTY SUTTON, Ohio
 LUIS V. GUTIERREZ, Illinois
 BRAD SHERMAN, California
 TAMMY BALDWIN, Wisconsin
 ANTHONY D. WEINER, New York
 ADAM B. SCHIFF, California
 ARTUR DAVIS, Alabama
 DEBBIE WASSERMAN SCHULTZ, Florida
 KEITH ELLISON, Minnesota

LAMAR S. SMITH, Texas
 RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin
 HOWARD COBLE, North Carolina
 ELTON GALLEGLY, California
 BOB GOODLATTE, Virginia
 STEVE CHABOT, Ohio
 DANIEL E. LUNGWEN, California
 CHRIS CANNON, Utah
 RIC KELLER, Florida
 DARRELL E. ISSA, California
 MIKE PENCE, Indiana
 J. RANDY FORBES, Virginia
 STEVE KING, Iowa
 TOM FEENEY, Florida
 TRENT FRANKS, Arizona
 LOUIE GOMPERT, Texas
 JIM JORDAN, Ohio

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING
 WASHINGTON, DC 20515-6216
 (202) 225-3951
<http://www.house.gov/judiciary>

FAX COVER SHEET

RELEASE

DATE: 10/9

TO: Hon. Ken Wainstein

FAX NO.: 202-353-9836

FROM: John Conyers Jr., Chairman Fax No.: (202) 225-7680

NUMBER OF PAGES IN THIS TRANSMISSION: 22 (including cover)

COMMENTS: _____

PLEASE CALL IF THERE ARE ANY PROBLEMS WITH THIS TRANSMISSION
 (202) 225-3951

JOHN CONYERS, JR., Michigan
CHAIRMAN

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOPGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SANCHEZ, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
BETTY CUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTHUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORDES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOMMERT, Texas
JIM JORDAN, Ohio

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951

<http://www.house.gov/judiciary>

October 9, 2007

Honorable Ken Wainstein
Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Wainstein:

Thank you for your recent appearance before the House Committee on the Judiciary. Your testimony on FISA and the Protect America Act was insightful and will assist the Committee in its consideration of this issue as we seek to fashion enhanced legislation.

Enclosed you will find additional questions from members of the Committee to supplement the information already provided at the September 18, 2007, hearing. As you will discover in the questions, there are some sets of questions that are specifically addressed to either you or Director Michael McConnell, while other questions request answers from both you and Director McConnell. You may choose whether to provide joint or separate answers to these latter questions. In addition, to the extent some questions (such as those initially contained in the September 11th letter to White House Counsel Fred Fielding) call for classified information, we are willing to make arrangements to receive the information in a manner that will protect its confidentiality.

Please deliver your written responses to the attention of Renata Strause of the House Committee on the Judiciary, 2138 Rayburn House Office Building, Washington, DC, 20515 no later than October 19, 2007. We would be pleased to accept answers on a 'rolling' basis in order to expedite the process. If you have any further questions or concerns, please contact Ms. Strause at (202) 225-3951.

Sincerely,



John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

**QUESTIONS FOR KEN WAINSTEIN AND MICHAEL McCONNELL
APPEARANCE BEFORE THE HOUSE JUDICIARY COMMITTEE**

September 18, 2007
2141 Rayburn House Office Building
11:00 a.m.

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.

The Role of the FISA Court (FISC) (Wainstein and McConnell)

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.
3. The Fourth Amendment requires that the government get a warrant before invading a person's privacy. Explain how the PAA's procedures can be constitutional without any court review whatsoever, other than minimization?

Minimization (Wainstein and McConnell)

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?
5. There is much more strict minimization under section 4 of section 1801(h). That section applies to pre-PAA FISA surveillance that is undertaken without a warrant and without judicial pre-approval. Under those circumstances, minimization is very strict: no contents of an innocent American's communication can be disclosed, disseminated, used, or even kept for longer than 72 hours without a FISA court determination or an AG determination that the information indicates a threat of death or serious bodily harm. If there is to be any warrantless surveillance spying on Americans' conversations, wouldn't it be more prudent to subject it to the strict minimization procedures of 1801(h)(4), which already

apply to other surveillance without a court order, and not the more lax minimization that has previously applied only when a court did provide a court order before Americans were spied on? If not, why not.

6. Minimization procedures have been keep secret for the last 30 years. There are serious concerns as to how we can be assured that minimization procedures are effective for protecting Americans' privacy if we cannot see them. Would you support making minimization procedures public?
 - a) If not, why not?
 - b) Would you support producing a redacted copy?
 - c) Minimization procedures only tell you what to do with US information after it is collected, therefore not revealing sources or methods. Thus, if do not support publicizing the procedures, on what do you base your objection?
7. Would you support legislation that would sequester communications to which an American is a party (and captured under this new program) that can only be used after an application to the FISA court? If not, why not?

Scope of PAA Section 105(B) (Wainstein and McConnell)

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

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 this transaction is “foreign intelligence information ... concerning persons reasonably believed to be outside the United States”? Please explain.
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.
14. Under Section 105(B) does the term “custodian” refer to anyone other than “custodians” of communications carriers?
 - 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.
 - 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.
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 such records to the Government with no other showing of cause that is subject to judicial review? Please explain.

Telecommunications Carriers Immunity Questions (Wainstein and McConnell)

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 is authorized and specifying 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?

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?
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?
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?
20. The pending cases against telecommunication companies are years away from final judgment. In light of that, would it be appropriate to have the discussion of retroactive immunity wait until we determine what actions actually occurred? If not, why not?
21. Would you support something more specific than the complete amnesty you propose in your draft legislation, like simply putting a damages cap on the claims? If not, why not?
22. In discussing the controversy over the PAA with the El Paso Times, DNI McConnell said "reverse targeting" was illegal, a violation of the Fourth Amendment, and that someone engaging in such offenses "could go to jail for that sort of thing." But wouldn't the immunity provisions recommended by the administration ensure that no one would go to jail for violations of the laws governing electronic surveillance for intelligence purposes?

Scope of Authority under the PAA (Wainstein and McConnell)

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?
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?
25. The Administration claims that it needs heightened access to communications because it

cannot instantaneously determine the location of each party.

- a) Phone companies are capable of determining international calls versus domestic calls, and charge more for the international calls. Would it be possible for the NSA to use similar technology? If not, why not?
- b) If it cannot be determined where either end of a call is, how can purely domestic to domestic communications be isolated?
- c) Is it possible to institute a program by which there is initial collection of calls, none of the content is accessed until the locations of the parties are determined, and then it can be retained and only the foreign to foreign calls used?

Metadata Collection (Wainstein and McConnell)

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.

FISA Exclusivity (Wainstein only)

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

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.
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 Federal Bureau of Investigation (Wainstein only)

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?
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?

Mismanagement in the Intelligence Community - - National Security Agency (McConnell only)

34. As the FISA Modernization Bill and the PAA were being debated in Congress, DNI McConnell and others in the administration suggested that advances in technology had created an "intelligence gap" which was making it more difficult for the intelligence community to keep America safe from terrorists. But according to a May 6, 2007 article in the Baltimore Sun, an internal NSA task force cited management problems as the cause of program upgrade delays, technology breakdowns and cost overruns, and called for a "fundamental change" in the way the NSA was managed. The report said NSA leadership "lacks vision and is unable to set objectives and meet them," and that NSA employees "do not trust our peers to deliver." These conclusions "are strikingly similar" to the conclusions of NSA management studies performed in 1999, yet even after 9/11 the fundamental changes recommended have not been made. Portions of this NSA task force report are not classified. Will you agree to release the unclassified portions of this report publicly and to the Committee?
35. Ensuring the proper management of intelligence would seem to be in many respects as important as increasing the authority to collect intelligence because, as the Joint

Intelligence Committee investigation into the 9/11 terrorist attacks showed, the NSA had intercepted communications linking the hijackers to terrorism long before 9/11 but that those intercepts, along with other critical pieces intelligence, were lost among the "vast streams" of data being collected. If we can assume that the NSA is collecting even more intelligence now than before 9/11, how can we be assured that the management problems at NSA are not hampering the intelligence community's ability to identify and understand which bits of intelligence are important and which are not? Please explain.

36. The September 14th Baltimore Sun report regarding a fire at an NSA "operations building" raises even more fundamental concerns about the NSA's ability to properly manage its operations. On August 6, 2007, right after the PAA was enacted, MSNBC and Newsweek reported that, "The National Security Agency is falling so far behind in upgrading its infrastructure to cope with the digital age that the agency has had problems with its electricity supply, forcing some offices to temporarily shut down." Please explain what steps are being taken in response to the reported fire and shutdown and other infrastructure and management problems.

German plot (McConnell only)

37. On September 10, you testified publicly before the Senate Homeland Security Committee that the temporary FISA changes due to the Protect America Act helped lead to the recent arrests of three Islamic militants accused of planning bomb attacks in Germany. But two days later, on September 12, you issued a contradictory statement, saying that "information contributing to the recent arrests was not collected under authorities provided by the Protect America Act." It has been publicly suggested that it was the pre-PAA FISA law, which you have criticized, that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act.
- a) Was your statement on September 10, claiming that the temporary Protect America Act helped lead to the German arrests, actually false?
 - b) Can you explain to us how it was that you came to give false information to the Senate Committee concerning the alleged contribution of the temporary Protect America Act to the German arrests?
 - c) Is it true that it was the pre-PAA FISA law that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act?

US persons "targeted" for surveillance (McConnell only)

38. In your recent interview with the El Paso Times, responding to a concern about "reverse

targeting,” you stated that there are “100 or less” instances where a U.S. person has been targeted for surveillance.

- a) Please explain how, when, why, and by whom it was decided to declassify that information and reveal it publicly.
- b) Over how long a period of time does that “100 or less” figure apply? For example, was it one year, five years, or since 9/11?

Declassification of Information (McConnell only)

39. At the hearing, you told Representative Scott that there is a process to declassify information and that ultimately it is the responsibility for the President to decide. Later in the hearing, you told Representative Sutton that when you did an interview you could declassify information because “it was a judgment call on your part.” Could you please explain the discrepancy between your two responses to similar questions?

Concerns About the House Bill (McConnell only)

40. During the hearing, in response to my question regarding the alleged 180 degree reversal of your position on the House bill regarding FISA this summer, you claimed that you had not changed your position but that once you had actually “reviewed the words” of the House bill, you could not accept it. Please explain specifically what problems you had with the “words” of the House bill.

Previous Problems Concerning Warrantless Surveillance and Minimization
(McConnell only)

41. In August 2005, the New York Times reported that John Bolton, then an official at the State Department, received summaries of intercepts that included conversations of “U.S. persons” and requested that the National Security Agency inform him who those persons were. Newsweek thereafter reported that from January 2004 to May 2005, the NSA had supplied the names of some 10,000 American citizens in this informal fashion to policy makers at many departments and law enforcement agencies. The former General Counsel at the NSA, Stewart Baker, was quoted as stating that the NSA would “typically ask why” disclosure was necessary, but “wouldn’t try to second guess” the rationale.
- a) What procedures are in place by entities such as the NSA that obtain summaries of conversations intercepted without a warrant to review the requests by other agencies, such as law enforcement agencies, to disclose

the identity of "U.S. persons" whose conversations are so intercepted without a warrant?

- 1) What showing, if any, is the requesting individual/agency required to make in order to obtain the identity of the U.S. person whose conversation was intercepted?
 - 2) Are any such requests denied, and, if so, in the past five years, state how many such requests have been denied?
- b) In the past five years, how many times have the summaries of such intercepted conversations been requested by and provided to the Office of the Vice President? To the Office of the President?
 - c) In the past five years, how many times have phone conversations of federally elected officials or their staff been intercepted under any surveillance program without a warrant? Do copies of those conversations still exist?
 - d) In the past five years, how many times have phone conversations of known members of the U.S. news media been intercepted without a warrant? Do copies of those conversations still exist?
 - e) In the past five years, how many times have phone conversations of attorneys in the United States been intercepted without a warrant? Do copies of those conversations still exist?
42. In 2006, Newsweek reported that the "NSA received—and fulfilled— between 3000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials ... that initially were deleted from raw intercept reports. . . . About one third of such disclosures were made to officials at the policymaking level." (See Mark Hosenball, "Spying, Giving Out U.S. Names," Newsweek, May 2, 2006).
- a) During the operation of the "terrorist surveillance program," prior to its disclosure in the New York Times in December 2005, how many "U.S. names" that were masked from transcripts of intercepts were disclosed (unmasked) to government entities that requested the identities?
 - b) What justification was required by a requestor to obtain the identity of the U.S. person on a minimized conversation?
 - c) What criteria, if any, were used to determine whether a request for the identity of a U.S. person on a minimized interception was appropriate or

whether the identity of the U.S. person was necessary for a legitimate intelligence or law enforcement purpose?

- d) If no justifications for identity information were required, and no criteria for review to determine the appropriateness of the request were in existence, then what purpose is served by the minimization procedures that mask a U.S. person's identity as a speaker on an intercepted phone call?
 - e) By name or position, which "policy makers" requested and received identity information of U.S. persons whose communications were intercepted?
43. The TSP was described in a Department of Justice (DOJ) "white paper" as "targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda" From the date of the inception of any warrantless interception program (approximately October 2001) through the 2007 decision to bring any such program under scrutiny of FISA, was the program ever broader to encompass any other international communications in addition to those reasonably believed to be linked to al Qaeda?
44. How many U.S. persons have been arrested or detained as a result of warrantless interceptions under the surveillance programs established by the President?
45. What is the date of the first document that purports to justify the warrantless surveillance program on the AUMF? How would you respond to claims that the AUMF rationale was a creation of Administration lawyers after the December 2005 New York Times article?
46. At any time from September 11, 2001 through December 2005, did the NSA obtain "trap and trace" or "pen register" information on the phones or telecommunications equipment of U.S. persons without court orders?
- a) If so, how many times?
 - b) If so, on what legal authority?
47. Since September 11, 2001, has law enforcement or the intelligence community conducted physical searches of the homes or businesses of U.S. citizens without warrants based on authorizations or approvals by the President or pursuant to a Presidentially authorized program?
48. Under the non-FISA warrantless interception programs, has law enforcement or the intelligence community deliberately caused the interception of purely domestic to domestic phone conversations without a FISA warrant? If so, what has been done with information so obtained?

49. Questions have been raised as to whether Christine Amanpour of CNN has ever had her telephone conversations intercepted by Administration surveillance programs. (See David Ensor, *NSA: Amanpour, Other CNN Reporters Not Targeted for Surveillance*, CNN, January 6, 2006). Has Ms. Amanpour ever been the target of warrantless surveillance – whether or not she was in the United States? Have any telephone conversations of Christine Amanpour been intercepted pursuant to any warrantless surveillance program?



U.S. Department of Justice

National Security Division

Assistant Attorney General

Washington, D.C. 20530

SEP 14 2007

RELEASE

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Reyes:

I write this letter in response to questions posed by you and other Members of the House Permanent Select Committee on Intelligence at its hearing on September 6, 2007, concerning the scope of the Protect America Act of 2007. You requested that certain answers given at that hearing be provided in writing and -- to the extent possible consistent with the national security -- in an unclassified format.

I appreciate your invitation to provide our thoughts on these matters as you evaluate the Protect America Act and consider our request to make the legislation permanent. I believe that this dialogue is a healthy process, and that it will help provide assurance to the American public and the Congress that the Act is a measured and sound approach to an important intelligence challenge.

The passage of the Protect America Act was a significant step forward for our national security. As this Committee is aware, sweeping changes in telecommunications technologies since the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978 expanded the scope of the statute substantially. As a result of these technological changes -- and not of any deliberate choice by the Congress -- the Executive Branch frequently was required to seek court approval, based upon a showing of probable cause, to conduct surveillance targeting terrorists and other foreign intelligence targets located overseas. This created a significant gap in our intelligence capabilities with no corresponding benefit to the civil liberties of persons in the United States.

By changing FISA's definition of electronic surveillance to clarify that the statute does not apply to surveillance directed at overseas targets, the Congress has enabled the Intelligence Community to close critical intelligence gaps, and the nation is already safer because of it. We urge the Congress to make the Protect America Act permanent, and also to enact the other important FISA reforms contained in the comprehensive FISA Modernization proposal we submitted to Congress earlier this year. It is especially imperative that Congress provide liability protection to companies that are alleged to have

assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

At the hearing last week, you and other Members of the Committee asked several specific questions concerning whether the Protect America Act hypothetically could authorize the Government to engage in certain intelligence activities that extend beyond those you contemplated when Congress passed the legislation. We appreciate the opportunity to provide you with answers, as these and other such questions have also been asked by other members of Congress and by members of the public.

While we understand the civil liberties concerns underlying these various questions, there are several reasons why this legislation does not give rise to these concerns. First, most of the hypotheticals we have heard are inconsistent with the plain language of the Protect America Act and the rest of the FISA statute. Second, we commit that we will not use the statute to undertake intelligence activities that extend beyond the clear purpose of the statute. And third, we will apply the statute in the full view of congressional oversight, as we intend to provide Congress with consistent and comprehensive insight into our implementation and use of this authority. As we have publicly committed, we will inform the full membership of the Intelligence and Judiciary Committees concerning the implementation of this new authority and the results of the reviews that this Division and the Office of the Director of National Intelligence are conducting to assess and ensure compliance by the implementing agencies; we will provide you copies of the written reports of those compliance reviews; and we will make ourselves available to brief you and your staffs about compliance and implementation on a monthly basis throughout this renewal period. In fact, representatives of the Executive Branch already have provided several detailed briefings to Committee Members and staff on the implementation of the Protect America Act since its passage. In addition, we have 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). With such comprehensive reporting to Congress, you and your colleagues will be able to see and assure yourselves that we are implementing this new authority appropriately, responsibly, and only in furtherance of the purposes underlying the statute.

I would like to address several of the hypothetical situations you and your colleagues raised at the hearing last week, and explain why we believe they will not arise under our implementation of the Protect America Act.

First, questions arose at the hearing concerning the Protect America Act's application to domestic communications, and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located

outside of the United States," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2) -- a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, several Members of the Committee asked whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the Government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows 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." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications -- further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

Third, a question was asked about whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, we do not think that this provision authorizes the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

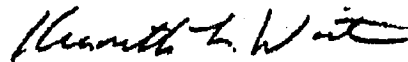
Fourth, and finally, it was suggested that this letter be used as an opportunity for the Executive Branch to allay concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA -- because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1) -- and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. Because it would remain a violation of FISA, the Government cannot -- and will not -- use this authority to engage in "reverse targeting."

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in "reverse targeting." If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target's calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target's communications.

Thank you again for the opportunity to appear at your hearing last week, and to provide these responses to your thoughtful questions. I hope you find this input helpful. Because we believe that these responses will likely be of interest to the Senate Select Committee on Intelligence and the Judiciary Committees, I have sent copies of this letter to the Chairman and Ranking Member of each of those committees.

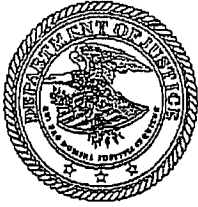
Please do not hesitate to call on me or my colleagues if we can be of further assistance as you consider FISA modernization and the renewal of the Protect America Act.

Sincerely,



Kenneth L. Wainstein
Assistant Attorney General

cc: Sen. Rockefeller
Sen. Bond
Sen. Leahy
Sen. Specter
Rep. Hoekstra
Rep. Conyers
Rep. Smith



Department of Justice

~~TOP SECRET//SI//NF//OC~~

SEGREGATE

STATEMENT OF

KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 20, 2007

~~TOP SECRET//SI//NF//OC~~

~~TOP SECRET//SI//NF//OC~~

STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 20, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA"). (U)

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before this Committee regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. We urge the Congress to make the Protect America Act permanent, and also to enact the other important reforms to FISA contained in the

~~TOP SECRET//SI//NF//OC~~

Administration's proposal. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans. (U)

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several concerns and misunderstandings that have arisen regarding the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation. (U)

The Need for Permanent FISA Modernization (U)

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."¹ The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents. (U)

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including

¹ H.R. Rep. No. 95-1283, pt. 1, at 22 (1978). (U)

most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."² (U)

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which Government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that its drafters never intended.) (U)

The original definition of electronic surveillance is the following:

(f) "Electronic surveillance" means-

- (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;

² *Id.* at 27. (U)

(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.³ (U)

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition 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." The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA's scope, period. (U)

Further analysis of that definitional language also demonstrates the opposite—that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as "radio" (vs. "wire") communications. Under the statutory definition, surveillance of these international/"radio"

³ 50 U.S.C. 1801 (f). (U)

communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of "electronic surveillance");⁴ or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that "both the sender and all intended recipients are in the United States").⁵ Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in "electronic surveillance" and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States. (U)

As satellite ("radio") gave way to transoceanic fiber optic cables ("wire") for the transmission of most international communications and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA's scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court

⁴ 50 U.S.C. 1801 (f)(1). (U)

⁵ At the time of FISA's enactment, the remaining two definitions of "electronic surveillance" did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to "wire communications," which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA's drafters explained was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." H.R. Rep. No. 95-1283 at 52. (U)

orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States. (U)

In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government's efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA's reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States. (U)

The legislative package we submitted in April proposed to fix this problem by amending the definition of "electronic surveillance" to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA's privacy protections on persons located in the United States. (U)

The Protect America Act of 2007 (U)

Although Congress has yet to conclude its consideration of the Administration's proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration's proposal. It is particularly critical that Congress

provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. (U)

By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation. (U)

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the information from or with the assistance of a communications service provider, custodian, or other person. (U)

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court.

The Act also provides that no cause of action may be brought in any court against any person for complying with a directive. (U)

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B concern persons reasonably believed to be outside the United States and therefore do not constitute electronic surveillance. The FISA Court then must review the Government's determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous. (U)

The following is an overview of the implementation of this authority to date. (U)

(1) Our Use of this New Authority (U)

The authority provided by the Act is an essential one and allowed us to close existing gaps in our foreign intelligence collection that were caused by FISA's outdated provisions. (U)

Exemption 1

b3

~~(TS//SI//OC//NF)~~

~~TOP SECRET//SI//NF//OC~~

Exemption 1

b3

~~(TS//SI//OC//NF)~~

~~TOP SECRET//SI//NF//OC~~

(2) Oversight of this New Authority (U)

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.
(U)

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel. (U)

The Department has completed two compliance reviews of the use of this new authority and is prepared to brief the Committee on the results of those reviews.

Exemption 1

b3

~~(TS//SI//OC//NF)~~

(3) Congressional Reporting About Our Use of this New Authority (U)

We intend to provide reporting to Congress about our implementation and use of this new authority that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period. (U)

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new

authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances. (U)

As I explained above, we already have completed two compliance reviews and are prepared to brief you on those reviews whenever it is convenient for you. (U)

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans. (U)

(4) Concerns and Misunderstandings about the New Authority (U)

I also want briefly to address some of the concerns and misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of the House Permanent Select Committee on Intelligence during a September 6, 2007, hearing, we sent a letter to that committee that clearly outlines the position of the Executive Branch on several such issues. We also sent a copy of that letter to this Committee. We hope that the letter dispels any concerns or misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement. (U)

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. As I

explained at a hearing of the House Judiciary Committee on September 18, 2007, the Act leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States. (U)

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States. (U)

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose. (U)

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order.

Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." I reiterated this conclusion at the House Judiciary Committee hearing on September 18, 2007—the statute simply does not authorize these activities. (U)

Section 105B was intended to provide a mechanism for the government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows 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." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3). (U)

Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of

private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes. (U)

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, this provision does not authorize the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so. (U)

Fourth, some have expressed concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were

communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach. (U)

Exemption 1

b3

~~(TS//SI//OC//NF)~~

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community's long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order 12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas. (U)

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal

investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures. (U)

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas. (U)

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the

silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place. (U)

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people. (U)

The FISA Modernization Proposal (U)

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. Second, Congress should provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. Third, it is important that Congress consider and ultimately pass other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of "agent of a foreign power" - - a category of individuals the Government may target with a FISA court order -- to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment

would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.

- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court.
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application. (U)

These and other sections of the proposal are detailed in the following section-by-section analysis. (U)

Section by Section Analysis (U)

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. Additionally, it is critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. This important provision is contained in section 408 of our proposal. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill -- both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent. (U)

Section 401 (U)

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus

FISA on the communications of individuals in the United States. As detailed above, when FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent. (U)

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed. (U)

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, "electronic surveillance" would encompass: "(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition

of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States. (U)

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.” (U)

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community’s ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but

his relationship to a foreign power is unclear.

Exemption 1

b3

It merits emphasis that the

Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances. ~~(TS//SI//OC//NF)~~ (U)

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute. (U)

Section 402 (U)

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which

these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today. (U)

It is important to note that the proposed amendment to this provision of FISA would not alter the types of "foreign powers" to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of "minimization procedures" referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection. (U)

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. This is a critical change that works hand in glove with the new definition of "electronic surveillance" in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of "electronic surveillance," certain activities that previously were "electronic surveillance" under

FISA would fall out of the statute's scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court. (U)

Section 403 (U)

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court. (U)

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction. The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of

foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable. (U)

Section 404 (U)

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives. (U)

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance. (U)

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications. (U)

Section 405 (U)

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above. (U)

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications. (U)

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to

obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm. (U)

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information. (U)

Section 406 (U)

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations

regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it "contains significant foreign intelligence information." This ensures that the Government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception. (U)

Section 406 also would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation. (U)

Section 407 (U)

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term "weapon of mass destruction." Subsection 407(a) also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of

mass destruction. Subsection 407(a) similarly amends the definition of "foreign intelligence information." Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction. (U)

Section 408 (U)

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided. (U)

Section 409 (U)

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process. (U)

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that *is about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard. (U)

Section 410 (U)

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches. (U)

Section 411 (U)

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national

security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States. (U)

Other Provisions (U)

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808). (U)

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration. It would allow for a smooth transition after the proposed changes take effect. (U)

Section 414 provides that any provision in sections 401 through 414 held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections. (U)

Conclusion (U)

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its

~~TOP SECRET//SI//NF//OC~~

original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We look forward to working with the Congress to achieve these critical goals. (U)

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions. (U)

~~TOP SECRET//SI//NF//OC~~



Department of Justice

~~TOP SECRET//SI//NF//OC~~

SEGREGATE

STATEMENT OF

KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 6, 2007

~~TOP SECRET//SI//NF//OC~~

~~TOP SECRET//SI//NF//OC~~

STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 6, 2007

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA"). (U)

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans. (U)

~~TOP SECRET//SI//NF//OC~~

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation. (U)

The Need for Permanent FISA Modernization (U)

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."¹ The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents. (U)

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."² (U)

¹ H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

² *Id.* at 27.

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which Government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that we submit its drafters never intended.) (U)

The original definition of electronic surveillance is the following:

(f) "Electronic surveillance" means-

- (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.³ (U)

³ 50 U.S.C. 1801 (f). (U)

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition 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." The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA's scope, period. (U)

Further analysis of that definitional language also demonstrates the opposite -- that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as "radio" (vs. "wire") communications. Under the statutory definition, surveillance of these "radio" - international communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of "electronic surveillance");⁴ or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that "both the sender and all intended recipients are in the United States").⁵ Therefore, if the Government in 1978 acquired communications by

⁴ 50 U.S.C. 1801 (f)(1). (U)

⁵ At the time of FISA's enactment, the remaining two definitions of "electronic surveillance" did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to "wire communications," which in 1978 carried a comparatively small number of transoceanic communications. The

targeting a foreign person overseas, it usually was not engaged in "electronic surveillance" and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States. (U)

As satellite gave way to wire and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA's scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States. In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government's efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA's reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States. (U)

The legislative package we submitted in April proposed to fix this problem by amending the definition of "electronic surveillance" to focus on *whose* communications are being

second definition, in section 1801(f)(4), was a residual definition that FISA's drafters explained was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." H.R. Rep. No. 95-1283 at 52. (U)

monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA's privacy protections on persons located in the United States. (U)

The Protect America Act of 2007 (U)

Although Congress has yet to conclude its consideration of that proposal, you took a significant step in the right direction by passing the Protect America Act last month. By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably believed to be outside the United States, the legislation clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation. (U)

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the

information from or with the assistance of a communications service provider or other person.

(U)

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive. (U)

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B do not constitute electronic surveillance. The FISA Court then must review the Government's determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous. (U)

The following is an overview of the implementation of this authority to date. (U)

(1) Our Use of this New Authority (U)

The authority provided by the Act is an essential one and we have acted swiftly to use this authority to protect the Nation. As a result, the Intelligence Community has effectively closed an intelligence gap identified by the DNI that was caused by FISA's outdated provisions.

(U)

~~TOP SECRET//SI//NF//OC~~

Exemption 1

b3

~~(TS//SI//OC//NF)~~ (U)

~~TOP SECRET//SI//NF//OC~~

(2) Oversight of this New Authority (U)

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA; (U)
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and, (U)
- subsequent reviews by the Department and ODNI at least once every 30 days. (U)

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel. (U)

As we explained in our letter to the Committee, the Department has completed its first compliance review of the use of this new authority and has offered to brief the Committee on the results of that review.

Exemption 1

b3

~~(TS//SI//OC//NF)~~ (U)

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide ample reporting to Congress about our implementation and use of this new authority. The Act provides that the Attorney General shall report concerning acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period. (U)

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our regular compliance reviews; (U)
- we will provide you copies of the written reports of those audits, with redactions as necessary to protect sources and methods; and, (U)
- we will give you update briefings every month on compliance matters and on implementation of this authority in general. (U)

As I stated above, we already have completed the first compliance review and are prepared to brief you on that review whenever it is convenient for you.

Exemption 1

b3

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans. (U)

(4) Misunderstandings about the New Authority (U)

I also want briefly to address some of the misunderstandings that have arisen regarding the Protect America Act. First, some have asked whether the wording of the Act would allow the Government to conduct warrantless electronic surveillance of individuals in the United States under the guise of an effort to obtain foreign intelligence information concerning individuals located outside the United States. That is not the case. If the target of the surveillance is located in the United States, the Government still generally is required -- as it has been since 1978 -- to obtain a court order to conduct the surveillance. (Certain pre-existing exceptions to the general requirement for a court order, such as the section 102(a) exception for official foreign powers, continue to apply.) Contrary to some reports, the new legislation does nothing to change FISA's prohibition against targeting a person in the United States for surveillance without a court order -- so-called "domestic warrantless wiretapping." (U)

We think that the provisions of new section 105B of FISA make this clear. To acquire foreign intelligence information under that section, the acquisition must not constitute "electronic surveillance" under FISA. The definition of "electronic surveillance" has not changed with regard to the interception of domestic communications. However, to the extent that the statute could be construed to allow acquisitions of domestic communications, we would be willing to consider alternative language. (U)

Second, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA's scope only foreign to

foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach. (U)

Exemption 1

b3

~~(TS//SI//OC//NF)~~ (U)

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community's long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order 12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas. (U)

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures. (U)

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas. (U)

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more

resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place. (U)

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people. (U)

The FISA Modernization Proposal (U)

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. We continue to believe that redefining the term "electronic surveillance" in a technology-neutral manner -- as we proposed in April -- is the best way to restore FISA to its original focus on surveillance activities that substantially implicate privacy interests in the United States and to reinstate the original carve-out for surveillance directed at persons overseas. (U)

We also believe that it is important that Congress consider and ultimately pass the other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of "agent of a foreign power" -
- a category of individuals the Government may target with a FISA court order --

to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm. (U)

- The bill would afford litigation protections to telecommunications companies that have allegedly provided the Government with critical assistance in its efforts to surveil terrorists and protect the nation since the September 11th terrorist attacks. (U)
- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court. (U)
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application. (U)

These and other sections of the proposal are detailed in the following section-by-section analysis. (U)

Section by Section Analysis (U)

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States, and the Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April. However, for purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill -- both major and minor. (U)

Section 401 (U)

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States. As detailed above, when FISA

was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent. (U)

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed. (U)

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, "electronic surveillance" would encompass: "(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the

sender and all intended recipients are reasonably believed to be located within the United States.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States. (U)

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.” (U)

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community’s ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear.

Exemption 1

b3

Exemption 1

b3

It merits emphasis that the

Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances. ~~(TS//SI//OC/NF)~~ (U)

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute. (U)

Section 402 (U)

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today. (U)

It is important to note that the proposed amendment to this provision of FISA would not alter the types of "foreign powers" to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of "minimization procedures" referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection. (U)

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. This is a critical change that works hand in glove with the new definition of "electronic surveillance" in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of "electronic surveillance," certain activities that previously were "electronic surveillance" under FISA would fall out of the statute's scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court. (U)

Section 403 (U)

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement -- that judges be drawn from seven different judicial circuits -- unnecessarily complicates the designation of judges for that important court. (U)

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction. The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable. (U)

Section 404 (U)

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements,

FISA today requires the Government to provide information that is not necessary to these objectives. (U)

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance. (U)

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate-

confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications. (U)

Section 405 (U)

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above. (U)

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications. (U)

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an

application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm. (U)

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information. (U)

Section 406 (U)

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it "contains significant foreign intelligence information." This ensures that the Government can retain and act upon valuable foreign

intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception. (U)

Section 406 also would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation. (U)

Section 407 (U)

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term "weapon of mass destruction." Subsection 407(a) also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of "foreign intelligence information." Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction. (U)

Section 408 (U)

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the

Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided. (U)

Section 409 (U)

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process. (U)

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard. (U)

Section 410 (U)

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change

would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches. (U)

Section 411 (U)

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States. (U)

Other Provisions (U)

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808). (U)

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration. It would allow for a smooth transition after the proposed changes take effect. (U)

Section 414 provides that any provision in sections 401 through 414 held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless

doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections. (U)

Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. The proposal that the Administration has submitted to the Congress in April would permanently restore FISA to its original focus on the protection of the privacy interests of Americans. This would improve our intelligence capabilities and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate such interests. We look forward to working with the Congress to achieve these critical goals. (U)

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions. (U)

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS
JOSEPH R. BIDEN, JR., DELAWARE
HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
RUSSELL D. FEINGOLD, WISCONSIN
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
BENJAMIN L. CARDIN, MARYLAND
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA
ORRIN G. HATCH, UTAH
CHARLES E. GRASSLEY, IOWA
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY D. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
SAM BROWNBACK, KANSAS
TOM COBURN, OKLAHOMA

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

1290 635
BW.
RECEIVED
NOV 13 2007
NOE
United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

November 13, 2007

Bryan A. Benczkowski
Principle Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 1601
Washington, DC 20530

RELEASE

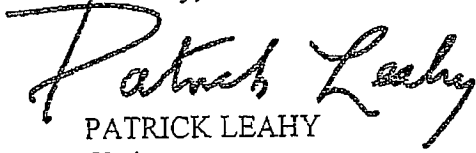
Dear Mr. Benczkowski:

Thank you for facilitating the testimony of Assistant Attorney General Kenneth L. Wainstein at the United States Senate Judiciary Committee hearing regarding "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" on October 31, 2007.

Enclosed are written questions from Committee members. In order to complete the hearing record, please send Mr. Wainstein's written responses as soon as possible and in no event later than Tuesday, November 27, 2007 to my office, attention Jennifer Price, Hearing Clerk, Senate Judiciary Committee, 224 Dirksen Senate Office Building, Washington, D.C., 20510. Please also send an electronic version of your responses to Jennifer_Price@judiciary-dem.senate.gov.

Again, thank you for your participation. If you have any questions, please contact Jennifer Price of my staff at (202) 224-7703.

Sincerely,


PATRICK LEAHY
Chairman

Questions of Senator Patrick J. Leahy
To Kenneth L. Wainstein

Definition of "Electronic Surveillance"

1. Both the Protect America Act and the Senate Intelligence Committee bill would change the definition in FISA of "electronic surveillance" to say that it does not include surveillance of a target overseas, even if that target is communicating with someone in the United States.

First, this is nonsensical – this clearly is electronic surveillance and to have a statute say that black is white is a bad practice. This change would also have consequences for other parts of the statute that use that definition. For example, there is a question about whether it renders inapplicable the civil and criminal liability provisions contained in FISA because those provisions are triggered by unauthorized "electronic surveillance."

Most importantly – it seems entirely unnecessary. The next part of the legislation would set up a new procedure for conducting the surveillance the government wants. There is no need to except it from the definition.

Q: Do you agree that if the statute sets up an alternative procedure to conduct the surveillance in the legislation, there is nothing in changing the definition that would add to the government's authority? If not, please explain in as much detail as possible what the definitional change accomplishes.

Immunity – Takings Issue

2. Retroactive immunity would strip away the rights of plaintiffs in those lawsuits to pursue on-going litigation that alleges violations of constitutional rights.

Q: Are there constitutional problems with doing this? Is it a “Taking” that violates the 5th amendment?

If there are no constitutional problems, can you point us to precedent where Congress has stepped in to quash on-going constitutional litigation?

If there are constitutional problems, do the retroactive immunity provisions contained in the Senate Intelligence bill address them?

Role of the FISA Court

The Senate Intelligence Committee bill would require the Government to submit targeting and minimization procedures to the FISA Court for the court’s review, but it would not require an up-front order from the FISA Court. The companies assisting with the surveillance would get their direction from the Attorney General and the DNI, not the Court.

Q: With the Senate Intelligence Committee bill, please describe your understanding of what power the FISA Court would have to stop the

Government from acquiring communications if it determines that the targeting or minimization procedures are flawed?

Immunity – Approval by Counsel to the President

4. The Report accompanying the Senate Intelligence Committee's legislation notes with respect to the "Terrorist Surveillance Program" that the Executive Branch provided the service providers with letters at regular intervals stating that the activities they were being asked to assist the government with had been deemed lawful by the Attorney General. The Report says this is true for all the letters except one. One letter stated that the Counsel to the President, not the Attorney General, had deemed the activities to be lawful.

Q: Even if you argue that the companies acted legally in compliance with FISA through most of this time, you cannot make that argument with respect to the period of time when Mr. Gonzales – then White House Counsel – approved the letters, can you?

Q: Given that the service providers provided assistance without regard for the statutory requirements for certification laid out in FISA and Title III, if we give them immunity now, how can we assure ourselves that they will follow the statutory requirements of FISA in the future and not just accept any written certification that the Administration gives them?

5. You stated more than once in your testimony that if any litigation should occur, it should be directed against the government, not the communications carriers who assisted the government. However, when I asked you how this would be done in light of the government's blanket assertions of state secrets, you responded, "there are many investigations going on right now about the propriety of what was done or not done under the Terrorist Surveillance Program. So in terms of accountability, if there is wrongdoing, that wrongdoing is being ferreted out in ways, very traditional ways, other than litigation."

Q: Please specify what particular avenues, other than litigation, you are suggesting we use to hold any wrongdoers involved in this matter accountable?

Senate Judiciary Committee Hearing on "FISA Amendments: How to Protect
Americans' Security and Privacy and Preserve the Rule of Law and Government
Accountability"

Wednesday, October 31, 2007

Questions Submitted by U.S. Senator Russell D. Feingold to Kenneth L. Wainstein
Assistant Attorney General

1. The Senate Intelligence Committee bill provides new authority for targeting individuals 'reasonably' believed to be located overseas. That determination of the target's physical location prevents warrantless wiretapping of Americans inside the United States, so it is critical that the government establish effective procedures to make sure it only uses this authority to target people overseas. Under the bill, the government starts using its targeting procedures before submitting them to the court for approval. If the court ultimately rejects those procedures, and determines that they are not reasonably designed to ensure that only overseas targets are wiretapped using these new authorities, what does the bill say would happen to all the communications involving U.S. persons that were acquired using the unlawful procedures before the court rejected them?
2. Does the Justice Department believe that private sector liability for unlawful surveillance plays any role in the enforcement of U.S. privacy laws and in providing disincentives to engage in unlawful behavior?
3. The Intelligence Committee Report on the FISA bill declassified for the first time the fact that after September 11, 2001, the administration provided letters to communications service providers seeking their assistance with communications intelligence activities authorized by the President. What is the Justice Department's position as to whether those letters comply with the statutory immunity provision in existing law, which is in Section 2511(2)(a) of Title 18?
4. Five weeks ago, I asked DNI McConnell whether the administration could provide this Committee with information about how much U.S. person information is looked at and how much is disseminated, under the new authorities provided in the Protect America Act. He told me that the information was already being compiled and should be ready in a matter of weeks. As far as I am aware, that information has not yet been provided. When will the Judiciary Committee get that information?
5. The Senate Intelligence Committee bill, like the Protect America Act, amends FISA's definition of "electronic surveillance." The consequences of that change are unclear. Does the Administration believe that it is necessary to amend that key definition? Would the legislation have the same effect if it added new authorities

but allowed the new definition of electronic surveillance in the Protect America Act to expire?

6. The Intelligence Committee bill permits the executive branch to begin surveillance based on its own procedures, and requires that they be submitted to the court only after the fact. What would be the harm in having the court review and approve the procedures prior to using them, with a provision for going forward without prior judicial review in an emergency?
7. Do you agree that there is a greater potential for intrusions on Americans' privacy rights, mistaken or otherwise, if the government is intercepting international communications in the United States, as opposed to when the interception occurs overseas?
8. Do the new authorities provided in the Intelligence Committee-passed FISA bill authorize the acquisition, from inside the United States, of any foreign-to-foreign communications in which a target is not a communicant? Do they authorize such acquisition of any foreign-to-domestic communications in which a target is not a communicant? Do they authorize such acquisition of any domestic-to-domestic communications in which a target is not a communicant?
9. As defined in Section 2510(15) of Title 18, the term "electronic communication service" is quite broad, and covers "any service which provides to users thereof the ability to send or receive wire or electronic communications." Does the Department of Justice believe that Title I of the FISA bill reported by the Senate Select Committee on Intelligence, S. 2248, which applies to providers of electronic communication services as defined in Section 2510 of Title 18, covers libraries that provide Internet access to their patrons or places of business that provide their staff with Internet access?
10. The Protect America Act contains a provision that permits communications service providers directed to conduct surveillance under that law to file a petition with the FISA Court challenging the legality of the directive.
 - a. Will you commit to notifying the Judiciary and Intelligence Committees if any such petitions are filed with the FISA Court challenging the Protect America Act, and will you share with those committees any court action, as well as the pleadings in those proceedings, redacted as necessary?
 - b. Will you commit to announcing, publicly, the fact that such a petition has been filed?

Senator Edward M. Kennedy
Questions for the Record
Senate Judiciary Committee hearing on "FISA Amendments: How to Protect Americans'
Security and Privacy and Preserve the Rule of Law and Government Accountability"
Held on October 31, 2007

*To Kenneth L. Wainstein, Acting Attorney General, National Security Division, U.S.
Department of Justice*

1. Thank you, Mr. Wainstein, for sharing your views on FISA with the members of this Committee. I regret that I was unable to attend the hearing in person. As the history of our surveillance laws teaches us, it's essential that we have a very careful and—to the fullest extent possible—public consideration of FISA legislation.

I was present at the creation of the FISA law, and I worked closely with a Republican Attorney General to draft its provisions. Together, we found a way to provide our intelligence agencies with the authority they needed, and also build in checks and balances to prevent abuse of that authority. FISA proved that we do not have to choose between civil liberties and national security.

Unfortunately, the Protect America Act was enacted this summer in a much less thoughtful process. It was negotiated in secret and at the last minute. The Administration issued dire threats that failure to enact the law before the August recess could lead to disaster. We need to correct that failure by engaging in a thorough, deliberative process before we enact more legislation.

It is encouraging that the Administration has finally agreed to share documents with members of this Committee and the Senate Intelligence Committee on its warrantless surveillance program. We had requested these documents for many months, because they are clearly relevant to the Administration's arguments on FISA.

But the Administration has not yet shared any documents with members of the House Judiciary or Intelligence Committees, whose new FISA bill it has criticized. This selective information-sharing is troubling because it suggests that the Administration will only work with those lawmakers who already agree with it.

Questions:

1. Why won't the Administration share the documents on its warrantless surveillance program with the House Intelligence and Judiciary Committees? Aren't these committees equally important players in this legislative debate?
2. White House press secretary Dana Perino was recently asked why the Administration was willing to share documents with the Senate Intelligence Committee but not with any others. She said it was because the Intelligence Committee's leaders "showed a willingness" to grant amnesty to the telecommunications companies. "Because they were

willing to do that," Ms. Perino said, "we were willing to show them some of the documents that they asked to see." Asked to clarify these disturbing comments several days later, a White House spokesman said that what the Administration did was "not exactly" a quid pro quo.

- a. Do you stand by these descriptions of the Administration's behavior?
 - b. These documents contain information that is clearly relevant to our responsibilities as lawmakers. How can you defend a policy of sharing them only with the committees that agree with the White House's preferences?
2. This Administration has asserted a view of executive power that is breathtaking in its scope. It has claimed the authority to wiretap Americans without warrants, despite the clear statement in FISA that it provides the "exclusive" means for conducting foreign intelligence surveillance. As we know from Justice Jackson's opinion in the Steel Seizure Cases, the President's authority is at its weakest when he acts contrary to a congressional enactment. Yet here, the President defied clear statutory language.

Questions:

1. If Congress enacts a FISA bill, will the President accept that he is bound by it? In particular, if we pass a bill that gives the President less power to conduct surveillance than he is now exercising, will he comply with it?
 2. If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?
 3. Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?
 4. Do you agree that new legislation should reaffirm that FISA is the sole means by which the Executive branch can conduct electronic surveillance outside of the criminal context?
3. As you know, the Administration is asking Congress to grant broad immunity for any past violations of the law by telecommunications companies that provided surveillance information. The Senate Intelligence Committee's bill grants this amnesty; the House Intelligence and Judiciary Committees' bill does not.

I have yet to hear a single good argument in favor of amnesty for the telecoms, but there are many reasons to be against it. Under FISA, communications carriers already have immunity from liability if they act pursuant to a court warrant or a certification from the Attorney General. In this way, FISA protects carriers who follow the law, while enlisting their help in protecting Americans' rights and the integrity of our electronic surveillance laws.

The Administration's proposal for immunity will help shield illegal activities from public scrutiny, but it will do nothing to protect our security or liberty. Instead, it will deprive plaintiffs of their rightful day in court, send the message that violations of FISA can be ignored, and undermine an important structural safeguard of our surveillance laws.

It's especially disturbing that the Administration apparently encouraged communications companies to break the law, and that those companies apparently went along. It's wrong to allow the Executive Branch to pick and choose which laws it obeys, and to ask others to help it break the law.

Questions:

1. Isn't it true that under FISA, companies that acted pursuant to a court order or an Attorney General certification already have immunity from liability?
 - a. Is it fair to say, then, that none of the telecoms being sued had one of these two documents, because if they did, they would already be off the hook?
2. In your testimony, you suggested that it would be "unfair" to the telecommunications companies to let the lawsuits proceed. I found this argument most unconvincing. Telecommunications companies have clear duties under FISA, and they have highly sophisticated lawyers who deal with these issues all the time. It is precisely because fairness and justice are so important to the American system of government that we ask an independent branch—the judiciary—to resolve such legal disputes. There is nothing fair about Congress stepping into ongoing lawsuits to decree victory for one side.
 - a. If a company violated its clear duties and conducted illegal spying, doesn't fairness demand that it face the consequences?
3. If Congress bails out any companies that may have broken the law, won't that set a bad precedent? What incentive will companies have in the future to follow the law and protect Americans' sensitive information?
4. If your concern is that carriers not be bankrupted, would you support something more specific than complete amnesty—for example, a cap on damages?
 - a. If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?
5. As you know, the President has said he will veto any FISA bill that does not grant retroactive immunity. At the same time, he and the Director of National Intelligence have said that if Congress does not make major changes to FISA, American lives will be sacrificed. If we take him at his word, then, the President is willing to let Americans die on behalf of the phone companies

- a. That's hard to believe. So why does the President insist on amnesty for the phone companies as a precondition for any FISA reform?

4. As you know, the Senate Select Committee on Intelligence recently reported a FISA bill, the "FISA Amendments Act of 2007," which has now come to this Committee on sequential referral. This bill would make major revisions to our surveillance laws in a variety of areas.

Although I appreciate the work of my colleagues on the Intelligence Committee in drafting this legislation, I have some concerns about their bill. For example:

- As I have said, the bill provides amnesty to telecommunications companies that may have broken the law in cooperating with the Administration on illegal surveillance, even though they already have broad immunity under current FISA law.
- The Intelligence Committee's bill redefines "electronic surveillance" in a way that is unnecessary and may have unintended consequences.
- The bill does not fully close the loophole left open by the Protect America Act, allowing warrantless interception of purely domestic communications.
- The bill does not require an independent review and report on the Administration's warrantless eavesdropping.
- The bill purports to eliminate the "reverse targeting" of Americans, but does not actually contain language to do so. There is nothing analogous to the House bill on reverse targeting, which prohibits such surveillance if "a significant purpose" is targeting someone in the United States.
- Court review occurs only after-the-fact, with no consequences if the court rejects the government's targeting or minimization procedures.

These are just a few of my concerns. But if I understand you correctly, you are generally supportive of the Intelligence Committee bill. Certainly, you seem to like it a lot more than the bill being considered by the House, which contains significantly greater protections for civil liberties.

Questions:

1. My understanding is that you are in favor of the way the Intelligence Committee bill redefines "electronic surveillance." In his written testimony, Mort Halperin described this change as "Alice in Wonderland": "It says that the language in FISA, which defines 'electronic surveillance,' means not what it clearly says, but what the current bill says."

- a. Why should we change the definition of "electronic surveillance"? It's a central term in FISA, and I see no good reason to replace it and open the door to many unintended consequences.
 - b. Mort Halperin has recommended that we strike out the part of the Intelligence Committee bill that redefines "electronic surveillance," and then change the requirements for the certification to be given to the FISA court to read "the surveillance is targeted at persons reasonably believed to be located outside the United States." How would this change affect your understanding of the legislation?
2. Unlike the House bill, the Intelligence Committee bill does not require prior judicial authorization before surveillance begins. This is a major departure from how FISA has always worked. It raises serious civil-liberties concerns, and makes it very difficult for courts to cut off surveillance that is illegal under the law. As Mort Halperin has stated: "By definition, if there is no emergency, there is time to go to the court and there is no reason to allow the executive branch to begin a surveillance without first having court approval. Requiring as a matter of routine that court approval must come first will assure that the executive branch gives the matter the full consideration that it deserves before starting a surveillance which will lead to the acquisition of many communications of persons in the United States and Americans abroad. . . . I cannot imagine any public policy argument to the contrary once one concedes that the court needs to play a role and there is an exception for emergencies with ample time limits."
 - a. How do you respond to Mr. Halperin's arguments?
 - b. Doesn't the abandonment of *before-the-fact* court review go against the basic promise of FISA that Americans will not have their communications acquired without a judge confirming that there is a legitimate reason to do so?
3. If you agree that purely domestic-to-domestic communications should never be acquired without a court order, would you support changes to the bill that would make this point 100% clear? As I read the bill, this is not as clearly prohibited as it could be.
4. If you agree that warrantless "reverse targeting" of Americans should never be allowed, would you support language in the bill to prohibit its use if "a significant purpose" is targeting someone in the United States?
 - a: If not, why not? The House bill contains this provision, and it's a sensible way to address the very serious "reverse targeting" concerns that will make Americans afraid for their rights.

U.S. SENATE COMMITTEE ON THE JUDICIARY
FISA HEARING — OCTOBER 31, 2007
QUESTIONS FOR THE RECORD FOR MR. WAINSTEIN
SUBMITTED BY SENATOR KYL

An amendment that was added to this bill in the Intelligence Committee by Senator Wyden adds a section to FISA that requires U.S. agents to obtain a warrant to conduct *overseas* surveillance of national-security threats if that surveillance targets a U.S. person.

1. Some advocates of this provision have described it as protecting the rights of U.S. citizens. The bill text, however, appears to cover "U.S. persons" — a category that FISA defines to even include U.S. green card holders. As I read the Wyden amendment, if a Pakistani national came to the United States as an adult for a few years, acquired a green card, and then returned to Pakistan and joined up with Al Qaeda, then under the Wyden amendment, this Pakistani national would be granted privacy rights under FISA that would bar the United States from monitoring his communications with the rest of Al Qaeda without first obtaining a warrant. Is that description accurate?

2. Would Middle Eastern governments be barred from monitoring the communications of this Pakistani green-card holder by any U.S. law if he were inside one of those Middle Eastern countries? In other words, under the Wyden amendment, would it be the case that the law would permit every government in the world — other than our own — to monitor the communications of this Pakistani Al Qaeda member when he is in the Middle East?

3A. Again, considering the hypothetical example of a Pakistani national who resides in Pakistan but has acquired a green card: under the Wyden amendment, the United States would be required to get court pre-approval and a warrant if it wanted to monitor this Pakistani in Pakistan in the course of a foreign intelligence investigation. Now suppose that the U.S. thought that this Pakistani green card holder were participating in drug smuggling in Pakistan and the FBI opened a criminal investigation. Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan in the course of a drug-smuggling criminal investigation?

B. What if this Pakistani national were believed to be involved in bribery of a public official while residing in Pakistan and the U.S. opened a criminal investigation of his activities. Would the U.S. be required to obtain a warrant to monitor such activities in Pakistan?

C. What if the U.S. thought that this green card holder were fencing stolen goods in Pakistan? Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan?

4. As I understand it, the Wyden amendment would apply not just when Pakistan-to-Afghanistan communications are routed through the U.S. Rather, it would apply whenever the activities of a U.S. green card holder are monitored overseas as part of a terrorism investigation. As a result, even if the U.S. were participating with the Pakistani government in an investigation inside Pakistan that targeted a Pakistani national who was a U.S. green-card holder, the U.S. would be required to report the investigation to the FISA court and seek a warrant.

I also understand that while many Middle Eastern governments cooperate with the United States in the war with Al Qaeda, many of these governments do not want other countries or radicalized elements of their own populations to know that they are helping the United States. As a result, many of these governments require that the fact of their cooperation with the United States or the details of joint counterterrorism operations not be disclosed outside of the U.S. intelligence community.

A. Would the Wyden amendment's requirement that the existence of intelligence investigations conducted entirely inside a foreign country be disclosed in U.S. court proceedings violate any of our information-sharing agreements with foreign intelligence services?

B. Should we expect that foreign intelligence services will refuse to share information or otherwise cooperate with the United States in the future if the Wyden amendment requires U.S. intelligence agencies to disseminate intelligence information outside of the intelligence community?

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS
JOSEPH R. BIDEN, JR., DELAWARE
HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
RUSSELL D. FEINGOLD, WISCONSIN
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
BENJAMIN L. CARDIN, MARYLAND
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA
ORRIN G. HATCH, UTAH
CHARLES E. GRASSLEY, IOWA
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
SAM BROWNBACK, KANSAS
TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

RELEASE

November 1, 2007

Bryan A. Benczkowski
Principle Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 1601
Washington, DC 20530

Dear Mr. Benczkowski:

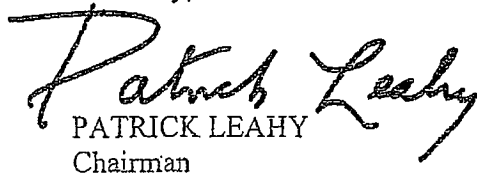
Thank you for facilitating the testimony of Assistant Attorney General Kenneth L. Wainstein's at the United States Senate Judiciary Committee hearing entitled "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" on October 31, 2007.

I have enclosed a copy of the unedited hearing transcript for Mr. Wainstein to review and make grammatical changes to his testimony, if needed. This is not the official hearing transcript and should not be copied or distributed under any circumstance.

Please mark any changes directly on the transcript and return it to my office, to the attention of Jennifer Price, Hearing Clerk, Senate Judiciary Committee, 224 Dirksen Senate Office Building, Washington, D.C., 20510. In order to complete the hearing record, please return this transcript with your changes as soon as possible and in no event later than Thursday, November 15, 2007.

Again, thank you for your participation. If you have any questions, please contact Jennifer Price of my staff at (202) 224-7703.

Sincerely,


PATRICK LEAHY
Chairman

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS
JOSEPH R. BIDEN, JR., DELAWARE
HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
RUSSELL D. FEINGOLD, WISCONSIN
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
BENJAMIN L. CARDIN, MARYLAND
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA
ORRIN G. HATCH, UTAH
CHARLES E. GRASSLEY, IOWA
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
SAM BROWNBACK, KANSAS
TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-5275

BRUCE A. COHEN, Chief Counsel and Staff Director
MICHAEL O'NEILL, Republican Chief Counsel and Staff Director

October 25, 2007

RELEASE

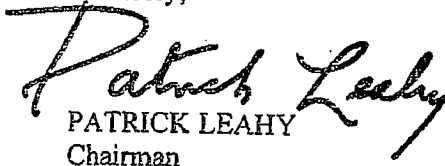
Bryan A. Benczkowski
Principle Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 1601
Washington, DC 20530

Dear Mr. Benczkowski:

Thank you for facilitating Assistant Attorney General Kenneth L. Wainstein's appearance and testimony at the Senate Committee on the Judiciary hearing on "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" scheduled for Wednesday, October 31, 2007, at 10:00 a.m. in room 226 of the Dirksen Senate Office Building.

Committee rules require that that written testimony be provided by 10:00 a.m., Tuesday afternoon, October 30. Please provide 75 hard copies of the written testimony and curriculum vitae by that time. Send the hard copies as soon as possible to the attention of Jennifer Price, Hearing Clerk, Senate Committee on the Judiciary, 224 Dirksen Senate Office Building, Washington, D.C. 20510. Please also send electronic copy of the testimony and a short biography via email to Jennifer_Price@judiciary-dem.senate.gov.

Sincerely,


PATRICK LEAHY
Chairman



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

RELEASE

OCT 3 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

We have provided for your review redacted copies of additional documents relating to the implementation of the Protect America Act of 2007 (Act), which amended the Foreign Intelligence Surveillance Act of 1978 (FISA). The Act moves FISA toward its original focus and provides critical new authority to conduct surveillance on foreign intelligence targets located overseas with more of the speed and agility necessary to safeguard the American people. We are grateful to Congress for identifying and remedying the vulnerability caused by the outdated FISA statute, and we are committed to ensuring that the use of the new authority is consistent with the Act and with the protection of the civil liberties and privacy of Americans.

Where necessary, we have made redactions to the documents to protect critical intelligence sources and methods. The highest classification level of these documents is Top Secret/Sensitive Compartmented Information (TS/SCI). As such, we have delivered the documents to the care of the Senate Security in S-407 of the Capitol.

We look forward to continuing to work with you on this critical issue. Please do not hesitate to contact this office if we may be of further assistance.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Cc: The Honorable Arlen Specter
Ranking Minority Member



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 2007

RELEASE

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

Dear Mr. Chairman:

We have provided for your review redacted copies of documents relating to the implementation of the Protect America Act of 2007 (Act), which amended the Foreign Intelligence Surveillance Act of 1978 (FISA). The Act moves FISA toward its original focus and provides critical new authority to conduct surveillance on foreign intelligence targets located overseas with more of the speed and agility necessary to safeguard the American people. We are grateful to Congress for identifying and remedying the vulnerability caused by the outdated FISA statute, and we are committed to ensuring that the use of the new authority is consistent with the Act and with the protection of the civil liberties and privacy of Americans.

Where necessary, we have made redactions to the documents to protect critical intelligence sources and methods. The highest classification level of these documents is Top Secret/Sensitive Compartmented Information (TS/SCI). As such, we have delivered the documents to the care of the Permanent Select Committee on Intelligence in H-405 of the Capitol.

We look forward to continuing to work with you on this critical issue. Please do not hesitate to contact this office if we may be of further assistance.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Cc: The Honorable Lamar Smith
Ranking Minority Member



U.S. Department of Justice
Office of Legislative Affairs

RELEASE

Office of the Assistant Attorney General

Washington, D.C. 20530

September 5, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable John D. Rockefeller IV
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

Dear Messrs. Chairmen:

On August 5, 2007, the President signed the Protect America Act of 2007 ("Act"), which amended the Foreign Intelligence Surveillance Act of 1978 (FISA). The Act moves FISA toward its original focus and provides critical new authority to conduct surveillance on foreign intelligence targets located overseas with more of the speed and agility necessary to safeguard the American people. We are grateful to Congress for identifying and remedying the vulnerability caused by the outdated FISA statute.

The Department of Justice is committed to ensuring that any use of the new authority is consistent with the Act and with the protection of the privacy and civil liberties of Americans. Use of this authority will be subject to rigorous oversight by any intelligence agency that uses it, by the Department, and by the Office of the Director of National Intelligence (ODNI). In addition, the Department will inform Congress of acquisitions authorized by the Attorney General and the Director of National Intelligence and of the reviews it conducts to assess compliance by the implementing agencies.

The implementation and use of this new authority will be subject to the following oversight measures:

- Regular reviews by the internal compliance office of any agency that exercises authority given it under section 105B of FISA;

- An audit/review by the Department and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures;
- Subsequent audit/reviews by the Department and ODNI at least once every thirty days;
- An agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

The Department's compliance audits/reviews will be conducted by attorneys of the Department's National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Officer.

The Department also appreciates the need for regular and meaningful reporting to Congress, so that Congress can fully understand our use of this surveillance authority as it considers its reauthorization. Accordingly, the Department will make itself available to brief and report to the committees listed below and their staff in the following ways:

- The Act requires the Attorney General to report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of noncompliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, noncompliance by a recipient of a directive, and the number of certifications issued during the reporting period.
- In addition to fulfilling these statutory requirements, Department representatives will be available to brief these committees after completing the first compliance review and after each subsequent review. At these briefings, Department representatives will report on the results of the compliance review, as well as incidents of noncompliance reported to it by an implementing agency. Such briefings will also include a discussion of what remedial efforts have been or will be undertaken in light of the findings of these reviews. The Department will make available to the committees any written reports of these reviews.

The Honorable Patrick J. Leahy, John D. Rockefeller IV, John Conyers, Jr., and Silvestre Reyes
Page Three

- Department representatives will be available to brief the committees on a monthly basis to update them on the results of further compliance reviews and generally on our use of the authority under section 105B.
- Because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

The Department is committed to working with the Congress to ensure that the authority granted by the Act is used to safeguard the nation's security in a manner consistent with the privacy and civil liberty interests of Americans. Please do not hesitate to contact this office if we may be of further assistance.

Sincerely,



Brian A. Benczkowski

Principal Deputy Assistant Attorney General

cc: The Honorable Arlen Specter
The Honorable Christopher S. Bond
The Honorable Lamar S. Smith
The Honorable Peter Hoekstra

Demers, John

From: Meadows, Bessie L
Sent: Wednesday, February 06, 2008 4:25 PM
To: Benczkowski, Brian A (OLA); Eisenberg, John; Demers, John
Cc: Gerry, Brett
Subject: RE: Fisa calls this afternoon

RELEASE

We are set to call Sen. Ben Nelson and Sen. Mark Pryor as soon as AG completes current call w/Cong. Scott

4:45 We are calling Sen. Ken Salazar

5:00 Sen. Tom Carper will call the AG

-----Original Message-----

From: Benczkowski, Brian A (OLA)
Sent: Wednesday, February 06, 2008 4:19 PM
To: Eisenberg, John; Demers, John
Cc: Meadows, Bessie L; Gerry, Brett
Subject: Fisa calls this afternoon

Can one or both of you AO the AGs fisa calls this afternoon? Bessie can give you details.



U.S. Department of Justice

Office of Legislative Affairs

RELEASE

Office of the Assistant Attorney General

Washington, D.C. 20530

October 12, 2007

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of Mr. Kenneth Wainstein, Assistant Attorney General, National Security Division, for the hearing held before the Committee on September 20, 2007, concerning the Foreign Intelligence Surveillance Act.

If we may be of further assistance, please feel free to contact this office.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosure



Department of Justice
RELEASE

STATEMENT OF

KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 6, 2007

**STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE**

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 6, 2007

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."¹ The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."²

¹ H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

² *Id.* at 27.

The mechanism by which Congress gave effect to this intent was its careful definition of “electronic surveillance,” the term that identifies which Government activities fall within FISA’s scope. This statutory definition is complicated and difficult to parse, in part because it defines “electronic surveillance” by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA’s use of technology-dependent provisions that has caused FISA to apply to activities today that we submit its drafters never intended.)

The original definition of electronic surveillance is the following:

(f) “Electronic surveillance” means-

- (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.³

³ 50 U.S.C. 1801 (f).

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition 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.” The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA’s scope, period.

Further analysis of that definitional language also demonstrates the opposite -- that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as “radio” (vs. “wire”) communications. Under the statutory definition, surveillance of these “radio” - international communications would become “electronic surveillance” only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of “electronic surveillance”);⁴ or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that “both the sender and all intended recipients are in the United States”).⁵ Therefore, if the Government in 1978 acquired communications by

⁴ 50 U.S.C. 1801 (f)(1).

⁵ At the time of FISA’s enactment, the remaining two definitions of “electronic surveillance” did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to “wire communications,” which in 1978 carried a comparatively small number of transoceanic communications. The

targeting a foreign person overseas, it usually was not engaged in “electronic surveillance” and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

As satellite gave way to wire and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA’s scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States. In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government’s efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA’s reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The legislative package we submitted in April proposed to fix this problem by amending the definition of “electronic surveillance” to focus on *whose* communications are being

second definition, in section 1801(f)(4), was a residual definition that FISA’s drafters explained was “not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States.” H.R. Rep. No. 95-1283 at 52.

monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA's privacy protections on persons located in the United States.

The Protect America Act of 2007

Although Congress has yet to conclude its consideration of that proposal, you took a significant step in the right direction by passing the Protect America Act last month. By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably believed to be outside the United States, the legislation clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the

information from or with the assistance of a communications service provider or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B do not constitute electronic surveillance. The FISA Court then must review the Government's determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us effectively to close an intelligence gap identified by the DNI that was caused by FISA's outdated provisions. I can discuss this in more detail in a classified setting.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already

have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

I can provide specific details of our oversight efforts in a classified setting.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide ample reporting to Congress about our implementation and use of this new authority. The Act provides that the Attorney General shall report concerning acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our regular compliance reviews;
- we will provide you copies of the written reports of those audits, with redactions as necessary to protect sources and methods; and,
- we will give you update briefings every month on compliance matters and on implementation of this authority in general.

As I stated above, we already have completed the first compliance review and are prepared to brief you on that review whenever it is convenient for you. The Government also has conducted an on-site briefing for the Committee's staff members regarding implementation of the Act.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Misunderstandings about the New Authority

I also want briefly to address some of the misunderstandings that have arisen regarding the Protect America Act. First, some have asked whether the wording of the Act would allow the Government to conduct warrantless electronic surveillance of individuals in the United States under the guise of an effort to obtain foreign intelligence information concerning individuals located outside the United States. That is not the case. If the target of the surveillance is located in the United States, the Government still generally is required -- as it has been since 1978 -- to obtain a court order to conduct the surveillance. (Certain pre-existing exceptions to the general

requirement for a court order, such as the section 102(a) exception for official foreign powers, continue to apply.) Contrary to some reports, the new legislation does nothing to change FISA's prohibition against targeting a person in the United States for surveillance without a court order - so-called "domestic warrantless wiretapping."

We think that the provisions of new section 105B of FISA make this clear. To acquire foreign intelligence information under that section, the acquisition must not constitute "electronic surveillance" under FISA. The definition of "electronic surveillance" has not changed with regard to the interception of domestic communications. However, to the extent that the statute could be construed to allow acquisitions of domestic communications, we would be willing to consider alternative language.

Second, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA's scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community's long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order

12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in

1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. We continue to believe that redefining the term "electronic surveillance" in a technology-neutral manner -- as we proposed in April -- is the best way to restore FISA to its original focus on surveillance activities that substantially implicate privacy interests in the United States and to reinstate the original carve-

out for surveillance directed at persons overseas.

We also believe that it is important that Congress consider and ultimately pass the other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of “agent of a foreign power” - - a category of individuals the Government may target with a FISA court order -- to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.
- The bill would afford litigation protections to telecommunications companies that have allegedly provided the Government with critical assistance in its efforts to surveil terrorists and protect the nation since the September 11th terrorist attacks.
- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court.
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States, and the Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April. However, for purposes of providing a complete review of the legislation proposed by the Administration in

April, the following is a short summary of each proposed change in the bill -- both major and minor.

Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States. As detailed above, when FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition,

“electronic surveillance” would encompass: “(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.”

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can

collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community's ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which

these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of “foreign powers” to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of “minimization procedures” referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute “electronic surveillance” under FISA. This is a critical change that works hand in glove with the new definition of “electronic surveillance” in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of “electronic surveillance,” certain activities that previously were “electronic surveillance” under FISA would fall out of the statute’s scope. This new provision would provide a mechanism for

the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of “electronic surveillance.” The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from “at least seven” of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court’s jurisdiction. The new provision would eliminate the restriction on the FISA Court’s jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

Section 404

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new

provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an

application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply

regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it “contains significant foreign intelligence information.” This ensures that the Government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 406 also would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term “weapon of mass destruction.” Subsection 407(a) also amends the section 101 definitions of “foreign power” and “agent of a foreign power” to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.” Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

Section 408

Section 408 would provide litigation protections to telecommunications companies who

are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that *is about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843)

regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches.

Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Other Provisions

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of

expiration. It would allow for a smooth transition after the proposed changes take effect.

Section 414 provides that any provision in sections 401 through 414 held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections.

Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. The proposal that the Administration has submitted to the Congress in April would permanently restore FISA to its original focus on the protection of the privacy interests of Americans. This would improve our intelligence capabilities and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate such interests. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.

Oral Statement of Kenneth L. Wainstein

on

The Foreign Intelligence Surveillance Act

before the

House Judiciary Committee

September 18, 2007

RELEASE

**ORAL STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE**

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

HOUSE JUDICIARY COMMITTEE

SEPTEMBER 18, 2007

Chairman Conyers, Ranking Member Smith, and Members of the Committee, thank you for this opportunity to testify concerning FISA modernization. I am proud to be here today to represent the Department of Justice and to discuss this important issue with you.

I'd like to take a few moments to explain why I think we need to make the Protect America Act permanent and enact other important reforms to FISA. To do that, I will go through my understanding of the history and evolution of FISA. I will then discuss how this evolution has ultimately impaired our intelligence capabilities, and brought us to the point where we need to modernize FISA on a permanent basis. Finally, I will briefly

describe the efforts we are making to ensure that the authorities you provided last month in the Protect America Act are implemented in a responsible and transparent manner.

The FISA Congress Intended: The Scope of FISA in 1978

In enacting FISA, the Congress of 1978 reacted to the abuses disclosed in the Church hearings that involved surveillance against Americans within the United States by establishing a regime of judicial review for foreign intelligence surveillance activities -- but not for all such activities; only for those that most substantially implicated the privacy interests of people in the United States. Congress designed a judicial review process that would apply primarily to surveillance activities within the United States -- where privacy interests are the most pronounced -- and not to overseas surveillance against foreign targets -- where cognizable privacy interests are minimal or non-existent.

Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," the term that identifies those Government activities that fall within the scope

of the statute and, by implication, those that fall outside it. Congress established this dichotomy by defining “electronic surveillance” by reference to the *manner* of the communication under surveillance -- by distinguishing between “wire” communications -- which included most of the local and domestic traffic in 1978 and were largely brought within the scope of the statute -- and “radio” communications -- which included most of the transoceanic traffic in that era and were largely left outside the scope of the statute. Based on the communications reality of that time, that dichotomy more or less accomplished the Congressional purpose of distinguishing between domestic communications that generally fell within FISA and foreign international communications that generally did not.

The Unintended Consequences of Technological Change

The revolution in communications technology since 1978 radically altered that reality and upset the careful balance in the statute. As a result, certain surveillance activities directed at persons overseas -- which were not intended to fall within FISA --

became subject to FISA, requiring us to seek court authorization before initiating surveillance and effectively conferring quasi-constitutional protections on terrorist suspects and other national security targets overseas. This process impaired our surveillance efforts and diverted resources that would have been better spent protecting the privacy interests of persons within the United States.

The Protect America Act of 2007

In April of this year, the Administration submitted to Congress a comprehensive proposal that would remedy this problem and provide a number of other important refinements to the FISA statute. While Congress has yet to act on the complete package we submitted, your passage of the temporary legislation in August was a significant step in the right direction. That legislation updated the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States, thereby restoring FISA to its original focus on domestic surveillance and allowing us the critical latitude to surveil overseas

terrorists and other national security threats without going through a lengthy court approval process.

By making this change, Congress enabled the Intelligence Community to close critical intelligence gaps, and the nation is already safer because of it. But the legislation only lasts for six months, and the new authority is scheduled to expire on February 5, 2008, absent reauthorization. We urge the Congress to make the Protect America Act permanent and to enact the other important FISA reforms contained in the comprehensive FISA Modernization proposal we submitted to Congress earlier this year. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the way of the September 11th attacks.

I see this renewal period from now until February, during which Congress considers permanently modernizing FISA, as an opportunity to do two things. First and foremost, it gives us the opportunity to demonstrate that we can use the authority provided by the Protect America Act responsibly, conscientiously and

effectively. That is an opportunity that we have already started to seize. As we explained in a letter we sent the Committee on September 5th, we have already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as on-site compliance reviews by a team from the Office of the Director of National Intelligence (ODNI) and the National Security Division of the Department of Justice. This DNI/NSD team has already completed its first audit, and it will complete further audits every 30 days during this interim period to ensure full compliance with the implementation procedures.

In that same letter, we also committed to providing Congress with comprehensive reports about how we are implementing this authority. We will make ourselves available to brief you and your staffs on the results of our regular compliance reviews; we will provide you copies of the written reports of those audits; and we will give you update briefings every month on compliance matters and on implementation of this authority in general. In fact, we have already provided implementation documents to the Committee. We

also are prepared to brief you on the first compliance review whenever it is convenient for you.

We are confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority, and that it will demonstrate that you made the absolutely right decision when you passed the Protect America Act last month.

This interim period also gives us one other opportunity -- the opportunity to engage in a serious debate and dialogue on this important issue. I feel strongly that American liberty and security were advanced by the Act, and that they will be further advanced by adoption of our comprehensive FISA Modernization proposal.

However, I recognize that this is a matter of significant and legitimate concern to many throughout our country. On Friday, we sent the Committee a copy of a letter that we sent to the Chairman of the House Permanent Select Committee on Intelligence addressing some common concerns and misunderstandings about the Act. We hope that the letter provides further assurance to

Congress and the American public that the Act is a measured and sound approach to an important intelligence challenge.

This Committee is wise to hold this hearing and to explore the various legislative options and their implications for national security and civil liberties. I am confident that, when those options and implications are subject to objective scrutiny and to honest debate, Congress and the American people will see both the wisdom and the importance of modernizing the FISA statute on a permanent basis.

Thank you again for the opportunity to appear before you. I look forward to answering your questions.

Oral Statement of Kenneth L. Wainstein

on

The Foreign Intelligence Surveillance Act

before the

Senate Select Committee on Intelligence

September 20, 2007

RELEASE

**ORAL STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE**

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 20, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, thank you for this opportunity to testify before you again concerning FISA modernization. I am proud to be here today to represent the Department of Justice and to discuss this important issue with you.

The Protect America Act is an important law that has allowed the Intelligence Community to close intelligence gaps caused by FISA's outdated provisions and it has already made our nation safer. In my statement this afternoon, I will briefly explain why I believe Congress should make the Protect America Act permanent

and enact other important reforms to FISA. I also will briefly describe the efforts we are making to ensure that the authorities you provided last month in the Protect America Act are implemented in a responsible and transparent manner.

Before I do that, I would like to express my appreciation for the opportunity we have been given to conduct briefings of Members and staff of this and other committees regarding the implementation and our interpretation of the Act. We value the opportunity to discuss these issues with you. We look forward to continuing our dialogue and working with this Committee as you consider making the Act permanent and enacting other reforms to FISA.

The FISA Congress Intended: The Scope of FISA in 1978

Let me turn now to why I believe the Protect America Act should be made permanent. As I explained in my testimony before this Committee in May, the judicial review process Congress designed in 1978 applied then primarily to surveillance activities within the United States -- where privacy interests are the most

pronounced -- and not to overseas surveillance against foreign targets -- where cognizable privacy interests are minimal or non-existent.

As the Committee is aware, Congress established this dichotomy by defining “electronic surveillance” in FISA by reference to the *manner* of the communication under surveillance -- by distinguishing between “wire” communications -- which included most of the local and domestic traffic in 1978 and were largely brought within the scope of the statute -- and “radio” communications -- which included most of the transoceanic traffic in that era and were largely left outside the scope of the statute.

The Unintended Consequences of Technological Change

As a result of the revolution in telecommunications technology in the last 29 years, certain surveillance activities directed at persons overseas -- which were not intended to fall within FISA -- became subject to FISA, requiring us to seek court authorization before initiating surveillance and effectively conferring quasi-constitutional protections on terrorist suspects and other national security targets

overseas. This process impaired our surveillance efforts and diverted resources that would have been better spent protecting the privacy interests of persons within the United States.

The Protect America Act of 2007

The Administration submitted to Congress a comprehensive proposal in April that would remedy this problem and provide a number of other important refinements to the FISA statute. While Congress has yet to act on the complete package we submitted, your passage of the Protect America Act was a significant step in the right direction. It has allowed the Intelligence Community to close critical intelligence gaps that were caused by the outdated provisions of FISA and has already made us safer.

But the legislation is scheduled to expire on February 1, 2008, absent reauthorization. We urge the Congress to make the Protect America Act permanent and to enact the other important FISA reforms contained in the comprehensive FISA Modernization proposal we submitted to Congress earlier this year. It is especially imperative that Congress provide liability protection to companies

that are alleged to have assisted the nation in the conduct of intelligence activities in the way of the September 11th attacks.

Implementation of the Protect America Act

I also want to assure the Committee that we recognize our responsibility to use the authority provided by the Protect America Act responsibly, conscientiously and effectively.

While we are steadfastly committed to protecting the nation from foreign terrorists and other national security threats through our foreign intelligence activities, we are equally committed to protecting the privacy interests of Americans. Importantly, both of these goals can be achieved under the framework Congress passed in the Protect America Act.

Our actions since Congress passed the Act demonstrate our commitment to the responsible implementation of the authority provided by the law. As we explained in a letter we sent the Committee on September 5th, we have already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as on-site compliance reviews by a

team from the Office of the Director of National Intelligence (ODNI) and the National Security Division of the Department of Justice.

This DNI/NSD team has already completed its first two compliance reviews, and it will complete further audits at least once every 30 days during this interim period to ensure full compliance with the implementation procedures.

In that same letter, we also committed to providing Congress with comprehensive reports about how we are implementing this authority that go well beyond what is required by the statute. We will make ourselves available to brief you and your staffs on the results of our regular compliance reviews; we will provide you copies of the written reports of those audits; and we will give you update briefings every month on compliance matters and on implementation of this authority in general. In fact, we have already provided implementation documents to the Committee. We also are prepared to brief you on the compliance reviews that have been conducted whenever it is convenient for you.

We are confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority, and that it will demonstrate that you made the absolutely right decision when you passed the Protect America Act last month.

We also recently addressed various concerns and misunderstandings that have arisen about the Act in a letter we sent to the House Intelligence Committee and we sent a copy of that letter to this Committee.

I feel strongly that American liberty and security were advanced by the Act, and that they will be further advanced by making the Act permanent and enacting the other important reforms in our comprehensive FISA Modernization proposal. However, I recognize that this is a matter of significant and legitimate concern to many throughout our country. We hope that the letter we sent the House Intelligence Committee on Friday provides further assurance to Congress and the American public

that the Act is a measured and sound approach to an important intelligence challenge.

This Committee is wise to hold this hearing and to explore the various legislative options and their implications for national security and civil liberties. I am confident that, when those options and implications are subject to objective scrutiny and to honest debate, Congress and the American people will see both the wisdom and the importance of modernizing the FISA statute on a permanent basis.

Thank you again for the opportunity to appear before you. I look forward to answering your questions.

RELEASE

Oral Statement of Kenneth L. Wainstein

on

The Foreign Intelligence Surveillance Act

before the

Senate Judiciary Committee

October 31, 2007

**ORAL STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE**

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

SENATE JUDICIARY COMMITTEE

OCTOBER 31, 2007

Chairman Leahy, Ranking Member Specter, and Members of the Committee, thank you for this opportunity to testify before you concerning FISA modernization. I am proud to be here today to represent the Department of Justice and to discuss this important issue with you.

I'd like to take a few minutes to discuss three points. First, why it is I believe Congress should permanently legislate the core provisions of the Protect America Act. Second, how it is that we've gone about implementing the Protect America Act with significant oversight and congressional reporting. And third, what our

preliminary views are on the thoughtful bipartisan bill reported out of the Senate Intelligence Committee two weeks ago, The FISA Amendments Act of 2007 -- S. 2248.

Before I do that, I'd like to express our appreciation for the attention Congress has given to the issue of FISA modernization. Congress has held numerous hearings and briefings on this issue over the past year or so. That process produced the Protect America Act--which was a significant step forward--and in the Senate it culminated in the strong bipartisan bill referred to this Committee, S. 2248, which was voted out of the Senate Intelligence Committee on a 13-2 vote. We applaud Congress for its initiative on this issue and its willingness to consult with us as it moves forward on FISA modernization.

Protect America Act

Let me turn now to why I believe that the core provisions of the Protect America Act need to be made permanent. The Government's foreign intelligence surveillance activities are vital to keeping the nation safe from international terrorists and other

national security threats. They provide critical information regarding terrorists who conspire to kill Americans at home and abroad--information that is key to tracking and disrupting terrorist operations. But, before the Protect America Act, our intelligence capabilities were significantly impaired by FISA's outdated legal framework.

Let me explain how that happened. The judicial review process under FISA that Congress designed in 1978 applied then primarily to surveillance activities within the United States -- where privacy interests are the most pronounced -- and not to overseas surveillance against foreign targets -- where cognizable privacy interests are minimal or non-existent. As a result of the revolution in telecommunications technology in the last 29 years, however, certain surveillance activities directed at persons overseas -- which were not originally intended to fall within FISA -- became subject to FISA, requiring us to seek court authorization before initiating surveillance and effectively conferring constitutional protections on terrorist suspects and other national security targets overseas. This

significantly hampered our intelligence collection efforts.

So we were faced with a situation in which more and more of our overseas surveillance was subject to the approval of the FISA Court. This was against the backdrop over those 29 years since FISA was passed of an increasing threat from international terrorists who take full advantage of modern communications to organize and command their international networks of terrorist operatives.

And it was this combination that brought us to the point where we needed to update FISA. In April of this year, the DNI submitted to Congress a comprehensive proposal to modernize the statute and I and other Executive Branch officials, including the DNI, testified before the Senate Intelligence Committee regarding that proposal in May.

Recognizing the need to address this issue, Congress passed the Protect America Act, and the President signed the Act on August 5, 2007. Within days, we implemented the new authority, and the DNI has announced that we have filled intelligence gaps that were caused by FISA's outdated provisions. To ensure that the Intelligence

Community can keep those gaps filled, we strongly urge Congress to reauthorize the core authorities provided by the Protect America Act.

Implementation of the Protect America Act

We have recognized from the outset that Congress would reauthorize this authority only if we could demonstrate to you and the American public that we can--and will--exercise this authority responsibly and conscientiously. To that end, we imposed oversight upon ourselves that is well beyond that required by the statute. We committed to congressional reporting substantially beyond the requirements of the statute and provided the Committee with documents regarding our implementation of the Act. We also publicly addressed various concerns about possible overbreadth of the statute, issuing a letter to this and other Committees explaining how we could not and would not use the authorities for purposes beyond those intended by Congress. In doing this, we have established a track record that provides a solid basis for permanent reauthorization of the Protect America Act authority.

Against that backdrop, the Senate Intelligence Committee recently voted out S. 2248 on a bipartisan 13-2 vote. While we are still reviewing it, we believe it is a balanced bill that includes many sound provisions that would allow our intelligence agencies to continue obtaining the information they need to protect the nation. That bill would allow our intelligence professionals to collect foreign intelligence against targets located outside the United States without obtaining prior court approval, and it provides retroactive immunity to electronic communication service providers that assisted the Government with a communications intelligence activity in the aftermath of September 11th. This immunity provision is necessary as a matter of fairness to those providers that stepped up to assist us, and it is critical to ensure their future cooperation. The bill also remedies the possible overbreadth concerns that some had regarding the Protect America Act and it includes significant oversight. We therefore are optimistic that S. 2248 will lead to a bill the President can sign.

We do, however, have concerns with certain provisions in S.

2248, which include the bill's sunset provision, and a provision which would extend the role of the FISA Court by requiring a court order approving acquisitions of foreign intelligence information from United States persons located outside the United States. We look forward to working with this Committee and Congress to address those concerns and to achieve lasting FISA reform.

Thank you again for the opportunity to appear before you. I look forward to answering your questions.