OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE INTELLIGENCE STAFF

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

APR 17 2008

Reference: DF-2008-00017

Dear Ms. Hofmann:

This is an interim response to your 21 December 2007 letter to the Office of the Director of National Intelligence, wherein you requested under the Freedom of Information Act (FOIA):

> **". . . records from September 1, 2007 concerning exchanges that Director McConnell or other ODNI officials have had with 1) members of the Senate or House of Representatives and 2) representatives of telecommunications companies concerning amendments to FISA..."**

We processed your request in accordance with the FOIA, 5 U.S.C. § 552, as amended. Enclosed are 19 documents, totaling approximately 77 pages, that have been found to be responsive to your request. Upon review, it has been determined that portions of eleven pages should be withheld on the basis of FOIA Exemption 2, 5 U.S.C. § 552(b)(2). ODNI will provide a final response to this request on 21 April 2008.

Sincerely,

Jennifer L Hudson
for

John F. Hackett
Director, Information Management Office

U. S. HOUSE OF REPRESENTATIVES

Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515
Phone: (202) 225-3951
Fax: (202) 225-7680
FACSIMILE COVER

TO: Hon. Mike McConnell

FAX NO: [redacted] # PAGES: 3 (including this page)

FROM:

____STACEY DANSKY	____LILLIAN GERMAN
____JONATHAN GODFREY	____SUSAN JENSEN
____BRANDON JOHNS	_X_ELLIOT MINCBERG
____MATTHEW MORGAN	____IRVING NATHAN
____DIANA OO	____MICHELLE PERSAUD
____ROBERT REED	____MELANIE ROUSELL
____GEORGE SLOVER	____SAM SOKOL
____GAYE STAFFORD	____RENATA STRAUSE
____DWIGHT SULLIVAN	____TERESA VEST
____LASHAWN WARREN	

COMMENTS: _____

If parts of this transmission are unclear or transmission was faulted, please call: (202) 225-3951.

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 15, 2007

The Honorable Michael "Mike" McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

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

Dear Director McConnell and Mr. Wainstein:

I am writing because of disturbing revelations over the past several days about warrantless Administration surveillance activities that allegedly occurred months before 9/11, and about claims that a company that did not participate in potentially unlawful surveillance activities may have been subject to retaliation by the Administration, including federal prosecution. According to news reports and papers filed with a federal court in Denver, as early as February, 2001, the NSA asked Qwest Communications and other telecommunications companies for some form of warrantless access to records concerning Americans' private communications. Although the precise nature and scope of the intercepted communications has not been revealed, one report suggests that it may have involved "monitoring long distance calls and Internet transmissions and other digital information." S. Shane, "Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11," *New York Times* (Oct. 14, 2007). Although Qwest apparently refused the request, which a former Qwest executive claims led to retaliation against him and his company, it is unknown what access to confidential customer information was provided by other telecommunications companies.

I appreciated your testimony several weeks ago on behalf of the Administration in connection with proposed improvements to the Foreign Intelligence Surveillance Act (FISA). It is crucial, however, that Congress be fully informed of all the Administration's surveillance activities involving telecommunications companies, particularly in light of the Administration's request that retroactive immunity from liability be provided to these companies and Administration officials. Accordingly, I ask that you provide the Committee with an immediate briefing on the facts behind these recent revelations, and that you then provide us with any documents concerning the nature and scope of these pre-9/11 activities and the legal basis for conducting them.

Please contact the Judiciary Committee office, 2138 Rayburn House Office Building, Washington, D.C. 20515 (Tel: 202-225-3951 Fax: 202-225-7680) as soon as possible. Thank you for your cooperation in this matter.

Sincerely,

John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

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

The Honorable Michael "Mike" McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director McConnell:

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 Assistant Attorney General Ken Wainstein, while other questions request answers from both you and Mr. Wainstein. 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

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?

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.

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?

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 2 4 2007

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

Dear Mr. Chairman:

I look forward to appearing before the Senate Judiciary Committee to discuss the Protect America Act (PAA) and the Foreign Intelligence Surveillance Act (FISA). However, I am concerned that the Committee does not have the appropriate witnesses joining me to ensure a full dialogue with the Committee on this important topic. The Department of Justice's Kenneth L. Wainstein, Assistant Attorney General of the National Security Division, should serve as a co-witness with me at this important hearing tomorrow, September 25th. My staff has been in discussion with your staff over the past week but apparently no agreement has been reached. Moreover, the Senate-confirmed General Counsel of the Office of the Director of National Intelligence, Benjamin A. Powell, should also appear as a witness to ensure a full, detailed discussion occurs at this hearing.

As the Nation's principal intelligence officer, I can and will address the intelligence requirements and capabilities needed regarding FISA. However, I am not a lawyer. It is likely some of the Judiciary Committee Members will ask questions about specific provisions in the Protect America Act (PAA); they will ask about the meaning behind specific words in the PAA in addition to FISA and its legal underpinnings. The Department of Justice is central to all discussions involving modification to this critical statute. Ken Wainstein has appeared with me in each of the FISA Hearings over the past several months and heads the office responsible for preparing and presenting FISA applications to the court. Ben Powell has also appeared with me at these Hearings and has been closely involved with your staff in all of the FISA discussions, and has been closely involved in the preparation of FISA proposals presented to Congress.

Finally, as you know Mr. Chairman, I have been personally criticized by some in the Congress and in the media for being too visible and central in the Congressional debates on FISA. That is not a role I have chosen, but if I am the single witness before the Judiciary Committee, I am being placed in the role as the lead advocate and perhaps even as a partisan-something I am not.

I appreciate your swift consideration of my request. If you have any questions on this matter, please contact me or my Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

J.M. McConnell

cc: The Honorable Arlen Specter

ES 2007-1083

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 24 2007

The Honorable Sheldon Whitehouse
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Senator Whitehouse:

Thank you for your recent letter. We deeply appreciate the time and effort you personally devoted to meeting with me and working to ensure we are able to effectively collect intelligence to protect our Nation while safeguarding the civil liberties of all Americans. We regret any misunderstanding created by the compressed timeframe and our actions.

As you noted, we did discuss a narrow proposal at our meeting on 11 July. Between 11 and 27 July, we met with many Members and staff to brief them on modernization of the Foreign Intelligence Surveillance Act (FISA) and better understand their views of the best way to proceed. While these meetings were proceeding, agencies were also considering narrowed statutory language that would ensure we closed and covered critical intelligence gaps. Our April 2007 proposal was in process for over a year and required clearance from several relevant agencies to ensure that the precise language did not harm our capabilities. As we have discussed, FISA is a very complex statute and a single word change can have major consequences. The narrow proposal of July 27 was the result of extracting relevant portions of our April proposal and adding new language. Although there was only a small amount of new text, the verbiage was significant. This change required experts to examine the impact of such an approach and compressed an interagency clearance process that generally takes many months to a matter of days. In the final weeks of this process, intelligence professionals worked around the clock to answer Member and staff questions, participate in briefings and discussion sessions, and at the same time examine several drafting options.

We do regret the misunderstandings that resulted from the urgency of the situation. We have always sought to work in an atmosphere of trust and cooperation and will continue to do so as this process moves forward. If you have any questions on this matter, please contact my Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted].

Sincerely,

J.M. McConnell

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

NOV 15 2007

The Honorable Edward M. Kennedy
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Kennedy:

Thank you for your letter of September 28, 2007, regarding the Senate Judiciary Committee hearing on September 25th and your questions on liability protection for those who are alleged to have assisted the Government following September 11, 2001. I appreciated the opportunity to testify before your committee on modernization of the Foreign Intelligence Surveillance Act (FISA). As stated during the hearing, we look forward to working with you on this critical legislation.

As you are aware, the "FISA Amendments Act of 2007," S. 2248, sponsored by the Chairman Rockefeller and Vice Chairman Bond of the Senate Select Committee on Intelligence (SSCI) is currently before your committee. This legislation received bipartisan support in the SSCI and contains a liability provision of the kind you discussed in your letter. Although some technical problems remain with S. 2248 as drafted by the SSCI, we believe that it is a balanced bill that includes many sound provisions that would allow the Intelligence Community (IC) to continue obtaining the information it needs to protect the nation. Moreover, the SSCI report on S. 2248 (S. Rep. No. 110-209 (2007)) addresses many of your concerns. We believe this report is one of the clearest unclassified articulations of the history of this issue and the need for liability protection to date.

Your letter also requested a response to several specific questions. First, you asked whether, before passage of the Protect America Act, parties who acted pursuant to a warrant or the Attorney General's certification had immunity from liability. From the perspective of the IC, as a general matter, anyone that assists the Government in defending our national security should be able to rely on the Government's assurances of legality. This position is consistent with the findings of the SSCI. After reviewing the relevant documents, that committee concluded that the private parties had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. S. Rep. at 10. Because that committee "concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received," the committee determined that the providers "should be entitled to protection from civil suit." S. Rep. at 11. The committee's measured judgment reflects the principle that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions.

However, in certain situations a party may be prevented from asserting a defense because the defense could divulge classified information. The United States generally does not confirm or deny allegations about intelligence activities. That is because disclosures tending to confirm or deny such allegations could reveal information about intelligence sources, methods, and capabilities, and could thereby cause exceptionally grave damage to the national security. The position of the Director of National Intelligence was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1101(a) and 1097, and charged with the responsibility for the protection of intelligence sources and methods. 50 U.S.C. § 403-1(i)(1). My predecessor, Ambassador John D. Negroponte, and I have both asserted the military and state secrets privilege in litigation concerning allegations of an alleged intelligence program.

You also asked why the parties should be granted liability protection if the Terrorist Surveillance Program was legal. As the SSCI noted in its report, the pending suits "seek hundreds of billions of dollars in damages from electronic communication service providers." S. Rep. at 8. We are fortunate that, although the threat from al Qaeda has persisted, we have not suffered another attack since September 11, 2001. Those who are alleged to have assisted the Government in preventing another attack deserve our gratitude rather than lawsuits that threaten crippling monetary liability.

Even if these suits are ultimately dismissed, litigation is likely to be protracted, with any additional disclosures resulting in renewed applications to the court to allow litigation to proceed. These disclosures and the resulting litigation have the potential to make public information that is appropriately classified. The SSCI recognized as much when it noted:

> [T]he identities of persons or entities who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence. . . . It would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance.

S. Rep. at 10. We face a sophisticated enemy that can be expected to use this information to their advantage. We should not allow them to benefit from needless litigation.

Allowing these lawsuits to continue could have a disastrous long-term effect on the IC. As a Director of the National Security Agency, a private sector consultant to the IC, and now the Director of National Intelligence, I understand that in order to accomplish our mission, we frequently need the sustained assistance of those outside of the Government. Companies may, in the future, be less willing to assist the Government if they face litigation each time they are alleged to have provided assistance. As the SSCI noted in its report, "electronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the IC cannot obtain the intelligence it needs without assistance from these companies." S. Rep. at 10. Litigation that is without merit may still harm our ability to protect vital sources and methods.

Your letter questions whether Congress, by enacting liability protection, would be endorsing certain activities and "the continued cover up of its details." The SSCI addressed this point and noted:

> [T]he Committee concluded that the providers, in the unique historical circumstances of the aftermath of September 11, 2001, had a good faith basis for responding to the requests for assistance they received. [S. 2248] makes no assessment about the legality of the President's program. It simply recognizes that, in the specific historical circumstances here, if the private sector relied on written representations that high-level Government officials had assessed the program to be legal, they acted in good faith and should be entitled to protection from civil suit.

S. Rep. at 11. Adopting a liability protection provision, like that contained in S. 2248, is a fundamental principle of fairness for those who helped protect American lives.

The IC has made every effort to respond to the numerous requests regarding the program, to include repeatedly sending its senior-most officials to testify about the program and providing as much documentation as possible, given the constraints attendant to a very sensitive intelligence program. The House Permanent Select Committee on Intelligence and the SSCI have been comprehensively briefed and provided with extensive documentation with respect to these activities, and are exercising thorough oversight in regard to intelligence matters. Indeed, we have made extraordinarily sensitive information available to the Senate Judiciary Committee, including authorizations, legal opinions, and other information.

Over the past year, in the interest of providing an extensive legislative record and allowing for public discussion and open legislative consideration of this issue, the IC has discussed in open settings extraordinary information dealing with our operations. Leaders of the IC have gone far further in open discussions than in any other time I can recall in my forty-year intelligence career. This will come at a price to our ability to collect vital foreign intelligence.

Finally, you asked about the precedent that would be set if Congress provides liability protection to companies "that may have broken the law." As a threshold matter, the Department of Justice has addressed the legality of the activities covered by S. 2248 and you are able to review that those activities were determined to be lawful. Nonetheless, the SSCI liability protection provision takes a narrow and balanced approach. This provision provides immunity only "for an intelligence activity involving communications that was designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, that was authorized in the period between September 11, 2001 and January 17, 2007, and that was described in written requests to the electronic communication service provider as authorized by the President and determined to be lawful." Sen. Rep. at 10. And the provision extends protection only to providers who acted in good faith.

The IC is concerned about the precedent that would be set in not providing liability protection. In determining whether to provide liability protection, the SSCI weighed the incentives such protection would provide.

> [E]lectronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies. Given the scope of the civil damages suits, and the current spotlight associated with providing any assistance to the intelligence community, the [SSCI] was concerned that, without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.

S. Rep. at 11.

We hope that this information is helpful to your inquiry. We are optimistic that S. 2248, as drafted by the SSCI, could lead to a bill the President can sign. We are concerned, however, that alternatives being considered do not include liability protection and contain various other problems, which could have adverse consequences for the IC. We look forward to working with the Congress to address these concerns and achieve lasting FISA reform. If you have any questions on this matter, please contact the Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted].

Sincerely,

J. M. McConnell

cc: The Honorable John D. Rockefeller IV
The Honorable Christopher S. Bond

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 0 7 2007

The Honorable Sheldon Whitehouse
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Senator Whitehouse:

Thank you for our 11 July 2007 meeting and for your letter of 27 July 2007, regarding the Administration's proposal to modernize the Foreign Intelligence Surveillance Act (FISA). We greatly appreciate the time and effort you and other Members of Congress spent working to close the gaps in our intelligence capability prior to the August recess. As you know, what passed was only a temporary measure (S.1927), and we look forward to working with you to make these and other important changes permanent.

During our meeting, we talked about the most essential aspects of FISA modernization and Intelligence Community (IC) needs in light of the heightened threat faced by the Nation. Our proposal reflecting these aspects was first transmitted to the Congress on 27 July 2007, with some technical changes following shortly thereafter, and is enclosed for your reference. The interim legislation that Congress ultimately passed left several critical issues, such as liability protection, unresolved. While not ideal, the Administration supported this approach to give the IC the tools it urgently needed to protect our Nation, pending continued discussion of those important additional issues. We look forward to working closely with you and your colleagues to address all of the changes the IC needs to truly modernize FISA for the 21st Century.

We hope that this information is helpful to your inquiry. If you have any questions on this matter, please contact the Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

J. M. McConnell

Enclosure: As stated.

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

Facsimile Cover Sheet

Please Deliver to: Hon. Michael McConnell

Fax No. [redacted]

From: CHAIRMAN PATRICK LEAHY

Phone: 202-224-5639

Number of Pages Including Cover: 2

Comments:

If there are any problems with this transmission, please call: 224-5639

THE DOCUMENT TRANSMITTED IS CONFIDENTIAL AND INTENDED FOR RECEIPT BY THE ABOVE NAMED INDIVIDUAL ONLY.

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

September 10, 2007

Hon. Michael McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director McConnell:

On August 5th President Bush signed legislation providing a temporary amendment to the Foreign Intelligence Surveillance Act (FISA). As you know, this legislation represents a very significant change to the process for approving and overseeing sensitive electronic surveillance. The legislation shifts oversight away from the FISA Court and into the hands of the Attorney General, in consultation with the Director of National Intelligence.

I invite you to testify before the Senate Judiciary Committee at a hearing on these matters on Tuesday, September 25, 2007 at 9:30 a.m. The Committee will be conducting oversight of the recent legislation. I am not convinced that its sweeping scope was necessary to address the national security concerns that the Administration had identified.

We also want to consider whether there are more effective mechanisms to assure appropriate oversight of surveillance involving U.S. persons. We need to restore the proper balance in order to maintain our security while preserving the constitutional rights of Americans and providing appropriate oversight of executive action involving private communications of Americans.

Sincerely,

PATRICK LEAHY
Chairman

cc: Hon. Arlen Specter

EDWARD M. KENNEDY
MASSACHUSETTS

United States Senate

WASHINGTON, DC 20510–2101

September 28, 2007

The Honorable J. M. McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Rm S513 DIAC
Washington, D.C. 20511

Dear Director McConnell:

This letter follows up on our exchange at the September 25 Senate Judiciary Committee hearing on FISA.

I appreciate your testifying at this hearing. As the history of FISA teaches us, it is essential to have careful and, to the fullest extent possible, public consideration of surveillance legislation. Too often, the Administration has sought to circumvent the process of deliberation and debate. My hope is that your appearance at this hearing marked the beginning of a new approach. I was gratified when I asked you whether you are "going to be working with this committee," and you replied, "Absolutely."

I have submitted for the record a number of questions, to which I look forward to your prompt response. In this letter, I wish to follow up on our discussion of the Administration's request for retroactive carrier immunity. As you know, the President is asking Congress to grant broad immunity for alleged violations of the law by communications companies that provided surveillance information. Even as he makes this request, however, the President will not tell us which carriers participated in the warrantless surveillance program, the nature and scope of their law-breaking, or why they deserve immunity for their actions.

The President's request is troubling. Under FISA, communications firms bear two responsibilities: to assist the government with lawful surveillance requests, and to resist the government on unlawful surveillance requests. When firms comply with lawful requests, they are granted immunity and financial compensation; when they comply with unlawful requests, they face legal liability. In this way, the private sector is enlisted to protect 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. Congress shouldn't immunize alleged lawbreakers for past actions without knowing what those lawbreakers did or why they did it.

At the hearing, I expressed my belief that it would be a "bad precedent" to grant full retroactive immunity for possible violations of FISA. I indicated that if the Administration's concern is that the companies involved may be bankrupted, then there are more reasonable legislative alternatives.

To clarify these basic issues, I hope you'll give detailed answers to the following questions:

- Isn't it true that, under FISA law before passage of the Protect America Act, carriers who acted pursuant to a warrant or the Attorney General's certification already had immunity from liability?
- If the warrantless surveillance program was legal as the Administration has claimed, what do carriers need retroactive immunity from?
- Wouldn't Congress be endorsing the warrantless spying program and the continued cover-up of its details by granting retroactive immunity?
- If Congress immunizes 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?

Thank you for your thoughts on these important matters. As I mentioned at the hearing, I worked closely with the Ford Administration to draft the original FISA in the late 1970s. Together, we found a way to provide our intelligence agencies with the authority they needed, while building in checks and balances to prevent its abuse. I hope to be able to work with you and your colleagues in the same open and collaborative fashion.

With respect and appreciation,

Sincerely,

Edward M. Kennedy

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

H-405, THE CAPITOL
WASHINGTON, DC 20515
(202) 225-7690

MICHAEL DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

October 25, 2007

Director Mike McConnell
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director McConnell: Mike,

We'll talk about this. T.P.

On May 18, 2006, I sent a letter to the President addressing three issues of great importance to me. The most important issue in the letter was to reemphasize that the Administration has the legal responsibility to "fully and currently" inform the House and Senate Intelligence Committees of its intelligence-related activities. I also expressed concern that Congress may not have been briefed about alleged activities and in other cases that Congress may not have received all information necessary to perform effective oversight of ongoing activities. Sadly, since that time things appear to have become worse, not better.

An unfortunate byproduct of learning through press accounts of alleged intelligence activities is the realization that the press could not have formulated many of the stories without the complicity of Administration officials within the Intelligence Community. Far too often detailed information provided to the news media appears selective, almost targeted for release by Administration officials. In some cases the information had not been briefed to the Congress and in other cases to only a few Members in Congress. I am particularly troubled by the fact that unofficial release or selective declassification of sensitive information is intended to influence public opinion more than it is to inform the public of the facts.

The House is currently considering a number of critical and highly sensitive intelligence and national security issues, including legislation relating to the Foreign Intelligence Surveillance Act, an intelligence authorization bill for Fiscal Year 2008, and consideration of both continuing threats from radical jihadists and other emergent situations in the Middle East.

As you know, members of the Committee who are briefed with respect to these issues take their responsibility to protect classified information extremely seriously. While the information that is provided to the Committee makes clear the steps that are necessary to protect national security and the American public, it has become in some cases extremely difficult to articulate the reasons for taking those steps in an informed way in the face of often groundless and unsubstantiated speculation by the press, interest groups, and members of the general public. Much of that speculation is formulated on account of public statements by you and other Administration officials, as well as authorized and unauthorized discussion of classified information to the news media. This "knowledge gap" that exists between what the Committee

knows, what the Committee does not know, and what has been unfortunately leaked to the news by Administration officials threatens to present serious obstacles with respect to critical issues.

Accordingly, I would appreciate further clarification both of the process that is used to approve public disclosure of classified or sensitive information in general, and of what specifically may be said publicly with respect to certain collection activities under the Foreign Intelligence Surveillance Act/Protect America Act.

With respect to FISA and the Protect America Act, we have made clear that the problem we face relates to targeting of foreign persons in foreign countries. In the absence of clear explanation of how such targeting could implicate the FISA process in the United States, there has been substantial – and completely unfounded and inaccurate – speculation that the collection activities primarily at issue in the PAA somehow implicate the civil liberties or constitutional rights of average Americans. You and I know that they do not do so, however it is difficult for Members of Congress to explain why this is not the case without describing sensitive intelligence sources and methods. This puts us at a significant disadvantage. Your efforts to further explain these issues in the public appear to have further confused the issue, and they certainly have left substantial uncertainty among Members of the Committee as to what may be discussed publicly.

Accordingly, I would like to obtain a full and detailed explanation of what aspects of the classified methods and legal issues have been determined to be declassified for public discussion, and of the parameters of issues and collection that continue to be considered classified.

More generally, as was discussed during your last appearance before the Committee, there is substantial uncertainty as to the process and criteria that have been used to approve for declassification a number of public statements by both you and General Hayden in recent weeks on highly sensitive issues, as well as what may be authorized disclosures by Administration officials to the news media. I have always operated – and will continue to operate – with the understanding that classified information is not for public release. However, there must be a common understanding going forward of the process for such declassifications, of how such declassification decisions are documented to prevent arbitrary and capricious disclosures, and of what information ultimately is deemed appropriate for public discussion. Accordingly, I would also appreciate a fuller explanation of how the recent public disclosures were managed with respect to these criteria, and how the Committee will be made aware of such decisions in the future.

I look forward to your response.

Sincerely,

Pete Hoekstra
Ranking Member

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

December 12, 2007

The Honorable Mike McConnell
Director of National Intelligence
Washington, DC 20511

Dear Mr. McConnell:

On behalf of the House Committee on the Judiciary, I want to express our sincere appreciation for your participation in the September 18, 2007, hearing concerning "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights." Your testimony was informative and will assist us in future deliberations on the important issues addressed during the hearing.

Also, please find a **verbatim** transcript of the hearing enclosed for your review. The Committee's Rule III (e) pertaining to the printing of transcripts is as follows:

> *The transcripts...shall be published in **verbatim form**, with the material requested for the record...as appropriate. Any requests to correct any errors, other than transcription, shall be appended to the record, and the appropriate place where the change is requested will be footnoted.*

Please return your transcript edits to the Committee on the Judiciary by December 21, 2007. Please send them to the Committee on the Judiciary, attention: Renata Strause, 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact Ms. Strause at (202) 225-3951.

Thank you again for your testimony.

Sincerely,

John Conyers, Jr.
Chairman

Enclosure

U.S. Senator Harry Reid

Senator for Nevada, Majority Leader

S-221 U.S. Capitol
Washington, DC 20510

PHONE(202) 224 – 3542
FAX (202) 228 - 2360

FAX TRANSMISSION

FAX TO:	Kathleen Turner, Director of Legislative Affairs, ODNI
FAX NUMBER:	[redacted]
FROM:	Office of Senate Majority Leader (Attn: Marcel Lettre/Ron Weich)
DATE:	17 Dec 2007
SUBJECT:	Attached letter
TOTAL PAGES (Including Cover):	2

COMMENTS:

HARRY REID
NEVADA

MAJORITY LEADER

United States Senate

WASHINGTON, DC 20510-7012

December 16, 2007

Admiral John M. McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Admiral McConnell:

As you know, the Senate will begin debate on the FISA Amendments Act of 2007 this week. Among the issues the Senate will consider is whether to grant retroactive immunity to telecommunications companies that are alleged to have assisted the government in its warrantless wiretapping program. You recently wrote in the New York Times that immunity is one of the three most critical issues in this bill.

We appreciate that you have provided access to the documents necessary for evaluation of this issue to the Senate Intelligence and Judiciary Committees, as each has in turn considered it. As the debate now moves to the full Senate, I believe it is of critical importance that all Senators who will be called upon to vote on this important question have an opportunity to review these key documents themselves so that they may draw their own conclusions. In my view, each sitting Senator has a constitutional right of access to these documents before voting on this matter.

I strongly urge you to make the documents previously provided to the Intelligence and Judiciary Committee regarding retroactive immunity available in a secure location to any Senator who wishes to review them during the floor debate. I appreciate your cooperation in this matter.

Sincerely,

Harry Reid

HARRY REID
Senate Majority Leader

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

Facsimile Cover Sheet

Please Deliver to: Hon. Michael McConnell

Fax No. [redacted]

From: Chairman Patrick Leahy

Phone: (202) 224-7703

Number of Pages Including Cover: 23

Comments:

If there are any problems with this transmission, please call: 224-7703

THE DOCUMENT TRANSMITTED IS CONFIDENTIAL AND INTENDED FOR RECEIPT BY THE ABOVE NAMED INDIVIDUAL ONLY.

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

October 9, 2007

Hon. Michael McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director McConnell:

Thank you for your testimony at the United States Senate Judiciary Committee hearing regarding "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?" on September 25, 2007.

Enclosed are written questions from Committee members. In order to complete the hearing record, please send your written responses as soon as possible and in no event later than Tuesday, October 23, 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

PATRICK LEAHY
Chairman

Senate Judiciary Committee
Hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Tuesday September 25, 2007

Questions Submitted by Chairman Patrick Leahy

Questions for Director of National Intelligence Michael McConnell

1. In your September 25 testimony and your September 20, 2007 letter to Senator Carl Levin, you say that you objected to S. 2011, the Rockefeller-Levin alternative to the Protect America Act, in part because you were given very little time to review it. You say that based on the quick review you were permitted, some provisions concerned you.

   With time to reflect, please identify which, if any, provisions of S. 2011 would interfere unacceptably with the flexibility the Intelligence Community's needs to conduct surveillance. Please give reasons and be as specific as possible. If there are changes to the offensive provisions that would eliminate your concerns while maintaining the provision's purpose, please identify those changes.

2. You testified that, although you "can't resolve the constitutional debate" about the President's authority to conduct surveillance outside of the statutory framework, you would exercise your own authority "consistent with this law" and would "cause the [Intelligence Community] to execute our authorities" in the same way.

   Do you commit that while you are Director of National Intelligence you will not permit the Intelligence Community to conduct electronic surveillance outside of the procedures and authorities provided by statute?

3. Please answer or clarify the following about minimization procedures under the Protect America Act:

   Have the minimization procedures used under the Protect America Act been submitted to the FISA Court?

   Would you support a statutory requirement that the FISA Court review the minimization procedures for the PAA?

   Has Congress received the minimization procedures used under the Protect America Act? Do you object to providing those procedures for review by members and cleared staff of this Committee?

   You say that "incidentally" intercepted communications of people within the United States that are determined to have no foreign intelligence value are

minimized and "expunged from the database." Can you clarify the process by which these documents are removed from the database?

Will you suggest a mechanism by which the FISA Court can assess the adequacy of minimization procedures under the PAA without unduly burdening the Intelligence Community in its surveillance activities?

4. You describe in your testimony the four tiers of oversight of the Protect America Act.

Can you please describe all oversight provided, inside or outside of the Executive Branch, of the scope of and protections for "incidental" interceptions of the communications of people within the United States. Provide as much detail as possible.

5. Senator Cardin asked you "Do you have any suggestions to us how we could set up a more effective involvement of the FISA Court" in the PAA process that would "give more comfort that we have in place the appropriate checks and balances without compromising the ability of your agency to go after the individual that you believe you should?"

Please answer Senator Cardin's question in as much detail as possible.

6. (a) Putting aside any constitutional or legal considerations, as DNI do you have any *national security* or *operational* objection to providing this Committee – with appropriate security measures to protect classified information – with the following:

   - Authorizations for the Terrorist Surveillance Program and related surveillance programs
   - All legal opinions related to those programs.
   - Certifications provided to any carriers who might have assisted the government in carrying out those programs?

   (b) Please provide those documents to this Committee.

7. Can the NSA determine, in real time or near real time, from where a cell call originates? Can it determine in real time or near real time the origin of an IP transmission?

Questions for James A. Baker

1. The Protect America Act changed the definition of electronic surveillance in FISA. What impact might this change have on FISA? Is the change necessary to accomplish the objectives of the PAA?

2. Please answer the following about the role of the FISA Court under the PAA:

Can Congress provide for more significant FISA Court role in oversight of the PAA without unduly burdening the Intelligence Community?

Does a "clearly erroneous" standard of review leave the Court a sufficient, substantive role?

Under the PAA, if the Court found the procedures that the Administration was using to determine "foreignness" were inadequate, what could it do?

Questions for James X. Dempsey

1. The Administration argues that the changes they sought with the Protect America Act are consistent with the original intent of Congress when it passed FISA in 1978 because FISA was intended to permit interception of all communications of Americans with persons abroad as long as individuals in the U.S. were not targets. They base this on the fact that FISA permitted the interception of all international radio communications, which, they say, carried almost all of the international calls at that time.

   Put aside whether this argument is factually correct. Should we be relying in our current discussion on the policy judgments of the Congress in 1978 about the need to protect international calls? With the enormous increase in Americans' international calls since 1978 as well as the advent of the Internet, email, and other advances in communications technology, would the intent of Congress in 1978 necessarily lead to the same judgment about protections for international communications?

2. In response to criticisms that the PAA allows the government to intercept the communications of Americans as much or for as long as it wants as long as those Americans are not targets, the Administration argues that they have no incentive to conduct "reverse targeting." They say that if they are interested in a person in the United States they will want to get a warrant so that they can intercept all of that person's calls.

   Does this response satisfy you?

Questions of Senator Dick Durbin
Senate Judiciary Committee Hearing
"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
September 25, 2007

Director of National Intelligence J. Michael McConnell

1. The Administration has taken the position that the President is not required to follow certain laws that he believes interfere with his power as Commander in Chief. Apparently that is the Administration's view of the Protect America Act. According to *The New York Times*:

> [S]enior Justice Department officials refused to commit the administration to adhering to the limits laid out in the new legislation and left open the possibility that the president could once again use what they have said in other instances is his constitutional authority to act outside the regulations set by Congress.

Will you pledge that the Intelligence Community will comply with the Protect America Act in all circumstances?

2. I received a letter from a constituent expressing concern that he might be subject to NSA surveillance because he corresponds by e-mail with a journalist in Iraq who writes for *The Chicago Tribune*. He wrote to the NSA to ask whether his communications have been subject to NSA surveillance. He received a response from the NSA that said the NSA "can neither confirm nor deny" that he has been subject to warrantless surveillance.

   a. Under the Protect America Act, could my constituent be subject to warrantless surveillance?
   b. Could American servicemembers overseas who call and e-mail their families in the U.S. be subject to warrantless surveillance under the Protect America Act?
   c. What assurances can you provide to innocent Americans that the NSA is not listening to their phone calls and reading their e-mails?

3. Some experts have concluded that the Protect America Act is so broadly drafted that it authorizes the government to gather the sensitive personal records of innocent American citizens in this country as long as you and the Attorney General certify the information "concern[s] persons reasonably believed to be outside the United States." Do you agree with this interpretation?

4. If the government does not intend to use the Protect America Act to seize the records of innocent Americans in the U.S., would you support revising the law to make this clear?

5. Some have proposed that the Protect America Act be revised as follows: the government would not be required to obtain a warrant for any surveillance where the target is reasonably believed to be outside the U.S., but the government would later be required to apply for a warrant if there is reason to believe that a "significant number" of intercepted communications involve a person who is in the U.S. Would you support revising the law in this way?

6. Some experts have proposed that the FISA court should review the government's surveillance procedures to ensure that they are reasonably likely to target non-U.S. persons outside the U.S. and collect foreign intelligence information. Would you support revising the law in this way?

Senate Judiciary Committee
Hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Tuesday, September 25, 2007

Questions Submitted by U.S. Senator Russell D. Feingold
to Director of National Intelligence J. Michael McConnell

1. In your opinion, should the Judiciary and Intelligence Committees be provided access to the Presidential Authorizations and Office of Legal Counsel opinions justifying the NSA warrantless wiretapping program, from 2001 to the present?

2. During the hearing, you testified that you could provide the Judiciary Committee, in a matter of weeks, with information about how much U.S. person information is looked at and disseminated under the new Protect America Act authorities. Please provide that information as soon as it becomes available.

3. The Protect America Act contains a provision that permits communications 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?

4. The Protect America Act authorizes surveillance directed at individuals 'reasonably' believed to be overseas, subject only to after-the-fact, "clear error" review by the FISA Court of the procedures for making that determination. If an American inside the United States were accidentally targeted under Protect America Act authorities, or if purely domestic communications were accidentally acquired, what happens to those communications?

5. The Protect America Act provides that FISA warrants are not required for surveillance "directed at" a person outside the United States. FISA uses the term "targeting," and according to the testimony of James Baker, intelligence professionals clearly understand what is meant by the term "targeting."

   a. What, if anything, is the difference between "directing" surveillance at a person, and "targeting" that person for surveillance?

b. If there is no difference, for the sake of clarity why not use the word "targeting"?

6. You have argued that the Protect America Act simply implements the intent of Congress in 1978, because FISA was originally intended to permit the Intelligence Community to intercept all communications of Americans with foreign countries without a court order, as long as individuals in the U.S. were not targets. Your support for this is that FISA permitted the interception of all international radio communications, and that, according to your testimony, "almost all" communications between the U.S. and other countries in 1978 were considered radio.

Two of the witnesses who testified on the second panel presented a different factual picture of the state of technology in the late 1970s. In their written testimony, Jim Baker, the former head of the Office of Intelligence and Policy Review at DOJ, and Jim Dempsey of the Center for Democracy & Technology, explain that international communications occurred both by satellite and undersea cable in the 1970s. In addition, FISA itself specifically required a warrant for some communications between the U.S. and overseas. Would you like to reconsider your assertion that FISA was originally intended to permit the government to intercept all international communications of individuals in the United States, without a warrant?

7. On its face, Section 105B of the Protect America Act is not mandatory. It is optional, meaning that the Intelligence Community could conduct surveillance of any individual overseas without fulfilling even the procedures in Section 105B. Do you agree that it is not a statutory requirement that the government follow the procedures laid out in Section 105B?

8. Does the President have authority to authorize electronic surveillance beyond what is permitted by FISA as amended by the Protect America Act?

9. Under the Protect America Act, what role is assigned to the FISA Court to play in developing and ensuring compliance with minimization procedures?

10. Is there 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?

11. Senator Leahy asked you about the minimization rules under the Protect America Act, and you told him that "if you're minimizing, you would take them out of the database." What are you referring to? Please clarify this statement.

Senator Edward M. Kennedy
Questions for the Record
From Senate Judiciary Committee hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Held on September 25, 2007

To Director of National Intelligence Mike McConnell

1. As the history of U.S. surveillance law teaches us, it is 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 tools they needed, while building in checks and balances to prevent abuse of those tools. FISA proved that often we do not have to choose between civil liberties and national security.

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

That process cannot begin if the Administration asks us to legislate in the dark. The Administration has failed to provide us with adequate information about its activities, the legal justifications for those activities, and the FISA court opinions that we are told make new legislation necessary. I hope this hearing will mark the beginning of the end of this stonewalling.

Questions:

- **Will you provide us with the information we need to make informed judgments about whether FISA needs to be reformed?**
- **Will you provide us with the legal justifications pursuant to which the Administration conducted warrantless surveillance of Americans?**
- **Will you provide us with details regarding the manner in which that surveillance was conducted?**

2. I was upset to read your comment in the *El Paso Times* that because we are debating FISA reform in Congress, "Americans are going to die." As you know, Congress takes great pains to protect classified secrets, and we are absolutely committed to protecting our country. Terrorists are well aware that their communications may be monitored.

Question:

- **Do you continue to maintain that "Americans are going to die" because of this debate?**

3. In the same *El Paso Times* interview, you discussed the two opinions by the FISA court that you say made new legislation necessary. You revealed that the first judge ruled that "what we needed to do we could do with an approval process that was at the summary level." You said, "the second judge looked at the same data and said well wait a minute I interpret the law, which is the FISA law, differently. And it came down to, if it's on a wire and it's foreign in a foreign country, you have to have a warrant . . . ."

In making these statements, you told the *El Paso Times* about FISA court opinions that the Administration has refused to share with Congress.

Questions:

- **Can you explain why you chose to leak these details?**
- **Do you stand by all the statements you made to the *El Paso Times*? For instance, do you stand by the statements that only about 100 people inside the U.S. are currently under surveillance by intelligence agencies and that "[i]t takes about 200 man hours to do one telephone number" for the FISA court?**
- **Will you make the two FISA court decisions you discussed available to the Committee?**

4. The Administration has asserted a view of executive power that is breathtaking in 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 President Bush defied clear statutory language.

It is disturbing that officials in the Administration find it so difficult to state that they will obey the law. The right and ability of Congress to be a check on the executive branch is a bedrock principle of our constitutional system. Yet the Administration is asking for our consent to a new law, while simultaneously insisting that no such consent is necessary.

Questions:

- **If we enact a new FISA bill, will the President and the Intelligence Community accept that they are bound by it? In particular, if we pass a bill that gives the President and the Intelligence Community less power to conduct surveillance than they are now exercising, will they comply with it?**
- **If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?**
- **Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?**
- **Do you agree that new legislation should reaffirm that FISA is the sole means by which the executive branch can intercept communications in the United States?**

5. The Administration is asking Congress to grant broad immunity for any past violations of the law by communications companies that provided surveillance information.

Once again, the enactment of FISA shows us the right way to handle this issue. Under that carefully drafted statute, communications carriers have immunity from liability if they act pursuant to a court warrant or a certification from the Attorney General that the matter falls within one of the statutory exceptions that permits surveillance without a warrant. In this way, FISA protects carriers who follow the law.

Unfortunately, the Administration is now seeking immunity for carriers that violated FISA. Worse, the Administration will not tell us which carriers participated in the warrantless surveillance program, the nature or scope of their law-breaking, or why they deserve immunity for their actions. Once again, the Administration is asking Congress to legislate in the dark.

I'm troubled that the Administration apparently encouraged communications companies to break the law, and that those companies apparently went along. Our democracy cannot tolerate an executive branch that picks and chooses which laws to obey, and then asks others to do the same. How can we in Congress, as responsible lawmakers, vote to immunize any persons or companies until we have a full explanation of what they did and why they did it?

Questions:

- **Isn't it true that carriers who acted pursuant to a warrant or the Attorney General's certification already have immunity from liability? If the warrantless surveillance program was legal as you have claimed, what do carriers need immunity from?**
- **Wouldn't Congress be endorsing the warrantless spying program by granting broad immunity?**
- **If Congress immunizes 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?**
- **If your concern is that carriers not be bankrupted, would you support something more specific than complete amnesty—for example, a cap on damages?**
    - **If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?**

6. The Protect America Act contains remarkably broad language. Under one provision, the Administration does not need a FISA warrant to intercept any communications "concerning persons reasonably believed to be outside the United States," so long as a significant purpose of the surveillance is to obtain foreign intelligence information—a term that sweeps much broader than terrorism—and reasonable procedures are in place.

As you know, there has been a great deal of confusion about what this provision authorizes, and many Americans are concerned that it goes too far. Along with Assistant Attorney General for National Security Kenneth Wainstein, you have tried to allay some of these concerns in public statements.

Specifically, both of you have said that, when properly read, the Protect America Act does *not* authorize:

1. warrantless surveillance of domestic-to-domestic communications (on the theory that these communications might "concern" a foreign target);
2. warrantless physical searches of the homes, mail, computers, or effects of individuals in the United States;
3. warrantless acquisition of the business records (including library and medical records) of individuals in the United States; or
4. "reverse targeting" of U.S. persons, in which the government does warrantless surveillance of a person overseas when its primary or coequal purpose is to surveil a person inside the United States with whom the overseas person is communicating.

These activities, you have said, are *not* lawful under the Act. My concern is that it is not sufficiently clear from the statute that these activities are prohibited.

Questions:

- **Since the Protect America Act is not clear about whether or not it prohibits such troubling practices, will you work with Congress on statutory language that clearly prohibits them?**
    - **If you will not make this commitment, why not? This is a statute that will remain in place after you have left office. Unless the statute is clear, how can we trust that the government will not try to read ambiguous provisions as broadly as it can?**

7. Several other features of the Protect America Act are troubling. There is little debate about what these features do. Their language is clear. It is the substance of these features that concerns me, because in my view they do not comply with the original intent of FISA.

Judicial review under the Protect America Act is extremely weak. The FISA court only gets to look at the procedures for ensuring that persons being targeted are outside the U.S. and that acquisitions conducted under Section 105B do not constitute electronic surveillance. This review occurs long after the fact, under a "clearly erroneous" standard.

This is far from the independent judicial review that FISA has always used to protect Americans. Some people resisted judicial oversight then just as they are resisting it now, but it has worked to safeguard Americans' security as well as their liberty, by ensuring that government surveillance activities are legal. The FISA court has been overseeing spying activities that touch American soil for nearly 30 years, without incident.

Also, congressional oversight under the Protect America Act is very weak. Reports are made to Congress semi-annually. The only information the Administration must provide is certain aggregate data (the number of certifications and directives issued during the reporting period) and descriptions of incidents of non-compliance. There is nothing in the statute to guarantee that Congress will learn how the statute is affecting Americans.

Further, there is no mechanism in the Act to ensure adequate protection for Americans' communications that are "incidentally" collected when the government is targeting someone overseas. For example, there is no requirement that these communications be minimized in any particular way. To the contrary, it seems that under the Act, the government can use and disseminate these communications as it wishes. There is no requirement that if a particular

American is "incidentally" wiretapped at great length, the government will at any point need to obtain a warrant.

Questions:

- Would you accept a stronger role for judicial review under new legislation?
  - For example, would you accept a role for the FISA court in reviewing the Intelligence Community's targeting and filtering procedures *before* these procedures go into effect?
  - Would you accept a standard of review higher than "clearly erroneous"?
  - There have been many complaints from the Administration that the FISA process is too burdensome. If this is one reason you want to minimize judicial oversight, can you explain why it would not meet your needs to have additional resources or more time to seek after-the-fact emergency warrants?
- Would you accept a stronger role for congressional review under new legislation?
  - For example, would you accept a requirement that the Administration report to Congress (in a classified setting, if necessary) how many Americans' communications were surveilled in the reporting period?
- Would you accept new rules that provide more protection for Americans whose communications are "incidentally" collected?
  - For example, would you accept special, enhanced minimization procedures for such collections?
  - Would you accept a requirement that if any particular American is "incidentally" surveilled in a sustained way, at some point a court warrant will be required?

8. One of the unfortunate consequences of the way the Protect America Act was passed is that there is still great confusion—even among members of Congress—about what it does and does not authorize. The statute itself is ambiguous in many places, and there is hardly any record in Congress to help interpret it. As Mort Halperin said to the House Committee on the Judiciary, "Congress enacted legislation the meaning of which is simply not deducible from the words in the text."

If the Administration had been more willing to work with Congress, we would have had an opportunity to ensure that the new legislation was clear, complied with the Constitution, and struck the proper balance between security and liberty. Instead, as Mr. Halperin said, "[t]he bipartisan and strong public support of the FISA was ruptured by the Administration's tactics."

I am not asking you at this time to go over every ambiguity in the statute, but I have questions about several provisions that are particularly unclear. It is important to learn what these provisions do and do not authorize in order to evaluate them effectively.

Questions:

- Section 105A of the Protect America Act refers to activities "directed at" persons abroad, while Section 105B refers to activities "concerning" such persons. Previous

drafts of the statute had used "directed at" in both sections. However, "concerning" appears to be a much broader term.
    - Why did the Administration insist on changing the language in Section 105B to "concerning"?
    - How do you plan on interpreting the "concerning" language?
- I am concerned about the phrase "other persons" in Section 105B(a)(3) of the Act. Who are these other persons that the Administration can now order to turn over communications? The Postal Service? Federal Express? Private individuals?
- I am also concerned about the potential breadth of Section 105B. Under the Protect America Act, would it be lawful to collect every communication from America to Germany—without a court warrant—if the purpose of this collection was to find one terrorist in Germany?
    - If not, please explain why this would be unlawful under the statute.
    - If this would be lawful, don't you find it troubling that potentially millions of communications could be intercepted in this way—without any court warrant—to find a single foreign target?
    - Will you work with Congress to find language that will place limits on overbroad warrantless surveillance?
- Does the Protect America Act cover stored communications—for instance, e-mails sitting in a person's mailbox—as well as real-time communications?
    - If not, where in the statute does it indicate that stored communications may not be collected under the Act?
    - If so, isn't this a significant change from the traditional FISA regime of intercepting real-time communications only?
- Under the Protect America Act, certifications are "not required to identify the specific facilities, places, premises, or property" that the government will be able to access.
    - Why not?
    - Does this mean that once it has a certification, the government will be able to collect any information it wants from a communications provider?

9. The Protect America Act gives the Administration great power to conduct warrantless surveillance of "persons reasonably believed to be outside the United States." Some of these persons might be U.S. citizens traveling or living abroad.

An Executive Order (12333) provides some limits on surveillance of U.S. citizens who are abroad. But it is just an Executive Order, and we all know that statutes can trump Executive Orders. Along with colleagues like Senator Whitehouse who have raised this issue, I am worried that under the Protect America Act, the Administration will be able to wiretap at will soldiers serving in Iraq, or Americans visiting relatives in other countries, or Americans studying or doing business abroad. Most Americans would be upset to learn that the government can do this.

Questions:

- If you agree that Americans who travel abroad do not sacrifice all their civil liberties and privacy rights at the border, will you work with Congress to make sure that new legislation recognizes privacy protections for Americans abroad?
- Do you believe that before the government can target a U.S. person abroad, a court warrant should be required?
    - If not, why should FISA's most central protection of Americans—that a warrant be required before their communications can intentionally be surveilled—suddenly disappear the moment they step over the border?
- If you are unwilling to require a FISA court warrant for surveillance that targets Americans abroad, would you be willing to codify in statute the standards and procedures of Executive Order 12333 for this surveillance?

To James X. Dempsey

1. Mr. Dempsey, in your remarks at the hearing you said, "I've heard a lot of progress being made and I've heard the outlines of an approach that is better than the approach in the Protect America Act," and then you outlined several elements of that approach. I found your analysis very interesting and illuminating.

Question:

- Can you please flesh out this approach? In particular, can you describe all the reforms that you think ought to be made to the Protect America Act, and indicate which ones you think would attract broad support and which ones would be controversial?

To all Panel II Witnesses (James A. Baker, James X. Dempsey, Suzanne E. Spaulding, and Bryan Cunningham)

1. One thing the Administration rarely mentions in its statements about the Protect America Act is the Fourth Amendment. Yet the Constitution is the supreme law of the land, and all legislation must comply with it. There is obviously some uncertainty in Supreme Court case law about the extent to which the Fourth Amendment limits electronic surveillance, but we know from cases like *Katz* and *Keith* that the Fourth Amendment does apply in many situations.

Questions:

- When Americans talk or e-mail with people overseas, does the Fourth Amendment provide any protection for their international communications?

- **In your view, does the Protect America Act comply with the Fourth Amendment? If not, what are the offending provisions?**
- **What role should the FISA court have in safeguarding Americans' Fourth Amendment rights?**

2. As you know, the Protect America Act weakens the role of the Foreign Intelligence Surveillance Court. For communications covered by the Act, the FISA court is permitted to conduct only a very general review of the government's collection procedures, long after the fact, under a "clearly erroneous" standard. That's a far cry from the central role that the Court has been playing under FISA.

The Administration has attempted to justify its undermining of the FISA court by claiming that more serious judicial review would be too burdensome, and that executive branch oversight is sufficient to make sure the law is not abused.

Questions:

- **How do you regard the Administration's arguments for why the FISA court should be marginalized?**
- **What role should judicial review have under any new legislation?**

3. Congressional oversight under the Protect America Act is also weak. Reports are made to Congress semi-annually. The only information that the Administration has to provide is the number of certifications and directives issued during the reporting period and descriptions of incidents of non-compliance.

Questions:

- **Are these reporting requirements adequate to ensure that Congress understands how the statute is affecting Americans and has the information necessary to fulfill its oversight responsibilities?**
- **What information does Congress need to conduct real oversight?**

4. The Administration is demanding that Congress grant retroactive immunity for communications service providers that complied with unlawful surveillance requests. Some of these companies apparently cooperated with the warrantless surveillance program, which violated FISA.

Questions:

- **How do you regard the Administration's argument that these companies must be granted full immunity or else they will go bankrupt? Aren't there other ways—such as a cap on damages—to prevent bankruptcy while still holding companies liable for violations of FISA?**

- **If bankruptcy is not the real issue, why is the Administration so adamant that retroactive immunity must be provided?**
- **Do you agree that provider liability is a key structural protection of FISA?**

5. Many of us are obviously concerned about the scope of the Protect America Act. The Act isn't clear in many respects, but it seems to authorize very broad warrantless surveillance—far broader than anything allowed under FISA.

Questions:

- **Under the Protect America Act, would it be lawful to collect every communication from America to Germany—without a court warrant—if the purpose of this collection was to find one terrorist in Germany?**
  - **How could the Act be amended to place some constraints on such activity?**
- **Does the Protect America Act cover stored communications—for instance, e-mails sitting in a person's mailbox—as well as real-time communications?**
  - **Is this a significant change in the law? Why does it matter?**
- **Why did the Administration insist on the phrase "concerning," rather than "directed at," when describing surveillance in Section 105B? Isn't "concerning" a significantly broader term?**
- **In general, would you say that the Protect America Act simply "modernizes" FISA to account for changes in technology and security threats? Or does the Act overturn FISA in key respects?**

6. The Administration has repeatedly claimed that the Protect America Act restores FISA's original intent. One aspect of this claim is that FISA was never intended to protect Americans who communicate with foreign targets. Director of National Intelligence McConnell has stated that "Congress crafted [FISA] specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target."

Questions:

- **Is this claim by the Administration correct?**
- **Even if the Administration's claim is correct, do you think it's appropriate to provide as little protection as this statute provides for Americans whose communications may be "incidentally" collected by the government?**

7. Under the Protect America Act, it is possible that millions of "incidental" communications between foreign targets and innocent American citizens will be collected by the government. Many of us are concerned that the Intelligence Community's minimization

procedures—the procedures that control what can be done with information after it has been collected—are insufficient to protect the privacy of these Americans.

Questions:

- To the best of your knowledge, what limits currently exist on the government's ability to store, analyze, and disseminate information it collects without a FISA warrant on Americans who were never a target?
- Should new legislation require stronger minimization procedures, either for all Americans' communications or at least for international communications that are "incidentally" collected?

8. It appears from the text of the Protect America Act that Americans who travel abroad are now extremely vulnerable to warrantless surveillance. When Americans travel out of the country, the Act suggests that the government can wiretap them—without any warrant—as long as a significant purpose of the surveillance is to obtain foreign intelligence information.

Questions:

- Is this correct?
- Can you explain what effect Executive Order 12333 has on the wiretapping of Americans abroad, and whether this Order will continue to have force under the Protect America Act?
- To protect the rights of Americans who travel abroad, should we require a warrant anytime the government wants to target a U.S. citizen?

9. We spent much of the hearing debating the Protect America Act, which is very controversial and troubling in itself. But the Administration is also asking for additional changes in the FISA law. For example, Director McConnell has asked for a variety of "streamlining" measures and for an extension of FISA's emergency provision from 72 hours to one week.

Questions:

- What do you think of these new requests?
- Beyond this debate we are having over FISA and the Protect America Act, what else does Congress need to do to ensure that our intelligence programs are as effective and responsible as possible?
    - It has been reported that the National Security Agency is having many problems with management and with the computational and translational aspects of intelligence analysis. Should these be priorities?
- Unfortunately, a majority of this Committee is hampered in this debate by not knowing precisely what we are fixing. Despite subpoenas, we have been denied the legal justifications for the warrantless surveillance program, and we have been denied access to the FISA court opinions that we are told made new legislation

necessary. We are being told we need to fix a problem whose nature and scope have not been revealed to us.

- Given the secrecy that enshrouds this entire debate, how would you recommend Congress fulfill its oversight responsibility?
- Do you think Congress should conduct a broader review of intelligence policy at this time?

"Strengthening FISA: Does the Protect America Act
Protect Americans' Civil Liberties and Enhance Security?"
September 25, 2007

Questions for the Record Submitted by Ranking Member Arlen Specter

Questions for Director of National Intelligence J. Michael McConnell

1. **How targeted is the surveillance being conducted pursuant to the Protect America Act?** In your August 22, 2007 interview with the *El Paso Times*, you said: "Now there's a sense that we're doing massive data mining. In fact, what we're doing is surgical. A telephone number is surgical. So, if you know what number, you can select it out." To the extent you can comment in an unclassified format, can you elaborate on how targeted the surveillance being pursued under the Protect America Act is?

2. **Do you interpret the Protect America Act to authorize a range of intelligence gathering activities?** In a July 31, 2007 letter to me, you indicated that the activity that has come to be known as the "Terrorist Surveillance Program" was just one "aspect" of the "various intelligence activities" authorized by the President after 9/11. Do you believe the Protect America Act encompasses or authorizes intelligence activities beyond the acquisition of communications that would constitute "electronic surveillance" under Section 101(f) of the Foreign Intelligence Surveillance Act (FISA), *but for* the exception to that definition created by new Section 105A of FISA?

3. **Protections for U.S. persons located overseas.** The Protect America Act refers to surveillance "directed at *a person* reasonably believed to be located outside of the United States," rather than limiting the scope of surveillance to *foreign persons*. Nevertheless, you have pointed out that Executive Order 12333, Section 2.5, already prohibits surveillance of U.S. persons overseas unless the Attorney General determines "in each case that there is probable cause to believe" the person is "a foreign power or an agent of a foreign power."

   At the hearing, you said you "would have no personal objection" to transferring the authority to approve surveillance of U.S. persons overseas to the Foreign Intelligence Surveillance Court, and codifying the required probable cause showing. Nevertheless, you cautioned against potential unintended consequences of such a change, and you highlighted the possible need to differentiate between U.S. persons and U.S. citizens.

   a. Having considered the issue, have you identified any potential concerns with such a change in the law? Does your analysis depend upon whether the collection of intelligence occurs inside the United States or outside the United States?

b. Can you elaborate on the implications of providing such protections to all U.S. persons, as compared to just U.S. citizens? Does the Executive Order recognize this distinction for purpose of Section 2.5?

4. **Use of the terms "concerning" and "directed at" in the Protect America Act.** In response to question from Sen. Feingold, you acknowledged some possible ambivalence about the choice of the terms "concerning" and "directed at" in different parts of the Protect America Act. Have you determined whether the terms "directed at" or "targeted at" could be used throughout the legislation without negative consequences for the collection of foreign intelligence?

Question for Bryan Cunningham

At the hearing, I asked you about the possibility of requiring the government to report back to the Foreign Intelligence Surveillance Court periodically about the surveillance conducted pursuant to the Protect America Act. You expressed concerns about having the court "evaluate the foreign intelligence value of the information" collected. Nevertheless, you suggested that it may be appropriate to have the court evaluate whether "the scope of the intercepts really worked" as contemplated. Could you elaborate on the type of review you would consider appropriate when the court is asked to reauthorize the government's surveillance procedures, including the appropriate standard of review?

Questions for Suzanne Spaulding

1. At the hearing, you testified that Congress should avoid creating exceptions to FISA's definition of "electronic surveillance," to prevent negating statutory protections linked to that definition. Nevertheless, given that the existing definition of electronic surveillance still distinguishes between "wire" and "radio" communications, would you support amending the definition to make it technology neutral?

2. In your testimony, you state that legislation reauthorizing or modifying the Protect America Act should limit the statute's scope to the collection of intelligence concerning terrorism, rather than the collection of foreign intelligence more broadly. DNI McConnell has testified, however, that our nation faces other equally pressing concerns, such as foreign intelligence involving the proliferation of weapons of mass destruction.

   a. Do you continue to believe that new legislation should not encompass foreign intelligence related to the proliferation of weapons of mass destruction and similar threats to our national security?

b. Are you worried that distinguishing between different categories of foreign intelligence might unnecessarily complicate the guidance and training provided to intelligence officers?

Question for James X. Dempsey

Your written testimony states: "a communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused." Would your analysis of the arguments for retroactive immunity change if the requests received by communications carriers were not "apparently illegal"? Would it be different, for example, if the carriers received a certification of the program's legality?

Questions for James A. Baker

1. In Jack Goldsmith's recent book, *The Terror Presidency: Law and Judgment Inside the Bush Administration*, Mr. Goldsmith writes: "Jim Baker analogizes the task of stopping our enemy to a goalie in a soccer game who 'must stop every shot, for the enemy wins if it scores a single goal.' The problem, Baker says, 'is that the goalie cannot see the ball—it is invisible. So are the players—he doesn't know how many there are, or where they are, or what they look like. He doesn't know where the sidelines are—they are blurry and constantly shifting, as are the rules of the game itself.'" (Emphasis added.)
   c. Is Mr. Goldsmith right to credit you, among others, with the soccer goalie analogy?
   d. What does the goalie analogy portend for our decisions about whether to renew the Protect America Act? Specifically, what are we to do when NSA analysts and DNI McConnell tell us that they cannot know in advance whether a terrorist overseas will call into the US?

2. Given your knowledge of the Foreign Intelligence Surveillance Court, how do you believe that court would react to an expansion of its jurisdiction to include approval of surveillance targeting U.S. persons overseas – if, for example, the authority granted to the Attorney General under Section 2.5 of Executive Order 12333 was transferred to the court by statute?

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 12, 2007

Chairman John D. Dingell
Chairman
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am writing on behalf of the Intelligence Community, with regard to the letter you recently sent to a number of telecommunications carriers seeking information concerning assistance that these carriers may have provided in response to requests from the Government.

Many of the questions in your letter are broadly worded and, as a result, may request the disclosure of information relating to intelligence activities. This information could be classified. The knowing or willful disclosure of classified information by private parties to unauthorized persons is prohibited by a number of federal statutes. *See, for example,* 18 U.S.C. § 798(a). The oversight of intelligence activities is conducted by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence consistent with the National Security Act of 1947 and long-standing practice. Members of those committees are informed about intelligence activities that may be implicated by your questions and exercise oversight as stated in the National Security Act of 1947.

We were also advised that the letter's discussion of National Security Letters (NSLs) may create some confusion. Your letter states that "[p]ursuant to the Foreign Intelligence Surveillance Act (FISA), the Federal Bureau of Investigation (FBI) may use NSLs to obtain, without court review, records from businesses, including telephone companies and Internet service providers." We understand that five statutes (not FISA) authorize the FBI and other government agencies, as appropriate, to request information from various entities, such as wire and electronic communications service providers, consumer reporting agencies, and financial institutions, in conducting authorized investigations, activities, and analysis. *See* 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709; 50 U.S.C. § 436. Requests under these statutes are often referred to as NSLs.

These NSL authorities are not part of the Foreign Intelligence Surveillance Act of 1978. There is, however, a separate portion of FISA that provides a mechanism for the FBI to obtain an order from the Foreign Intelligence Surveillance Court (FISC), or a United States magistrate judge designated pursuant to the statute, to require the production of certain business records for foreign intelligence purposes. *See* 50 U.S.C. § 1861. I understand that this provision does not permit the Government to require production of such materials without a court order. Orders issued pursuant to this statute are typically referred to as section 215 or business record orders. It

is important to distinguish between these very different types of authorities because of the different standards and procedures applicable to each.

It is important to distinguish between these provisions, as well as other aspects of FISA, to avoid confusion. For example, the letter seeks information regarding the number of instances when telecommunications carriers have "been requested to commence a wiretap . . . without an NSL, where the entity seeking such information has subsequently received authorization." We are advised that NSLs cannot be used to commence a wiretap under FISA. As a result, it will be difficult for telecommunications providers to provide any useful information in response to such a question—requests by the Government to conduct electronic surveillance would have taken place "without an NSL." Similar problems arise with answering a number of the other questions in the letter.

Telecommunications providers, as well as other private parties, provide invaluable assistance to the Government's efforts to enforce the laws that protect all of us, from laws that protect the most vulnerable from child pornographers to those that protect the nation from terrorists. Private parties should be thanked for their efforts. Instead, companies have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. It is fundamentally unfair for these companies to continue to face the costly burden of litigation on these matters. The nation cannot expect cooperation if it is not willing to ensure that companies alleged to cooperate with the Government will be protected from litigation. Moreover, such litigation risks the disclosure of state secrets and thus could damage our national interests. Therefore, it is 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.

If you have any additional questions on this matter, please do not hesitate to contact me.

Sincerely,

Kathleen Turner

Kathleen Turner
Director of Legislative Affairs

cc: The Honorable Ed Markey
The Honorable Bart Stupak

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

OCT 30 2007

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

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

Dear Chairman Rockefeller and Chairman Reyes:

This letter presents the views of the Administration on H.R. 2082 as passed by the House of Representatives and the Senate Amendment thereto (referred to below as S.1538), entitled the "Intelligence Authorization Act for Fiscal Year 2008.". We appreciate the Committees' inclusion in their respective bills of many of the provisions contained in the Administration's draft bill, and thank you for your efforts on behalf of the Intelligence Community (IC). The Senate bill, in particular, contains provisions that support the mission and function of the Office of the Director of National Intelligence (ODNI) and the IC. We also recognize that the Senate eliminated several controversial provisions from its bill prior to passage.

Unfortunately, there remain provisions in both bills and their classified annexes that cause the Administration concern. Indeed, certain provisions in both bills are inconsistent with the protection of intelligence sources and methods, the need for effective conduct of intelligence activities, the recommendations of the 9/11 commission, and the need for legislative-executive cooperation with respect to U.S. intelligence activities. For the reasons stated below and identified in my classified letter, dated September 10, 2007, the Administration would have difficulty supporting a bill that does not satisfactorily address these concerns, omits the important authorities granted to the DNI in the Senate bill, or contains harmful restrictions on the DNI's ability to manage his office and the IC. In particular, should the final authorization not satisfactorily address the provisions of significant concern to the Administration described immediately below, the President's senior advisors would recommend that he veto the bill.

Provisions of Significant Concern

The Administration was pleased that Congress addressed the need to modernize the Foreign Intelligence Surveillance Act (FISA) by passing the Protect America Act (PAA), S. 1927, and looks forward to working with the Congress on making these changes permanent. We must continue to ensure that the IC is gathering critical foreign intelligence to protect America from another attack, consistent with the protection of privacy and civil liberties. We are further

encouraged by the positive steps taken recently by the Senate Select Committee on Intelligence (SSCI). The SSCI's "FISA Amendments Act of 2007" has strong bipartisan support and, although aspects of this bill are problematic, the Administration appreciates the SSCI's efforts to fix collection problems related to foreign intelligence surveillance. However, provisions included in both intelligence authorization bills raise issues that are counterproductive to a constructive dialogue on this important issue. We believe that a comprehensive discussion of these provisions is best held in the context of the FISA Amendments Act.

- Section 504 of H.R. 2082, which purports to reiterate that FISA is the exclusive means by which electronic surveillance may be conducted for gathering foreign intelligence information raises constitutional questions. The bill purports to reiterate that FISA is the exclusive means by which electronic surveillance may be conducted for gathering foreign intelligence information. FISA presently contains an exclusivity provision and the inclusion of an additional and broader exclusivity provision raises unnecessary and highly complex legal questions. Nonetheless, the Administration has agreed to discuss inclusion of an appropriately drafted exclusive means provision in connection with the SSCI's FISA Amendments Act. The provision, as drafted in H.R. 2082, however, suffers from technical problems that could disrupt the effective conduct of intelligence activities. Similarly, it would limit our ability to protect the Nation by prohibiting the Government from using the provisions of chapter 119 of title 18 of the U.S. Code for gathering foreign intelligence information. Finally, the provision in H.R. 2082, by requiring the Congress to be extremely clear and precise in the face of a crisis, creates a potential for uncertainty in the IC at a time when clarity is most needed.

- In the context of the Intelligence Authorization Act, the Administration also strongly opposes section 315 of S. 1538, which would amend the FISA to require the Attorney General to submit a copy of any order issued by the FISA Court or the FISA Court of Review that includes significant construction or interpretation of the Act. Section 315, as amended, would also require the Attorney General to submit copies of all decisions, orders, and opinions issued by both courts. We are concerned that neither section contains provisions for redacting or summarizing particularly sensitive information, which may be included in these materials. Accordingly, these provisions may undermine the President's responsibility to protect access to certain kinds of national security information. As much of this information is already provided to the committees in the form of a semi-annual report, and to the intelligence committees in briefings, we believe that reporting on FISA matters is appropriately left to established channels. Despite our concerns, the Administration is prepared to discuss this provision further with Congress in the context of the SSCI's FISA Amendments Act.

Contrary to the 9/11 Commission recommendations, the Senate bill would create no less than 5 new Senate-confirmed positions, increasing the potential for delay in filling critical leadership positions in the IC. As the Commission noted, new intelligence officials need to assume their responsibilities as quickly as possible to avoid disruptions in the national security policymaking process.

- The Administration supports the creation of a statutory Deputy Director of the Central Intelligence Agency, but opposes the requirement in section 421 of both S. 1538 and H.R. 2082 that the nominee be confirmed by the Senate.

- Likewise, section 434 of S. 1538, would create a statutory Director of the National Security Agency (NSA), Director of the National Geospatial-Intelligence Agency (NGA), and Director of the National Reconnaissance Office (NRO) to be appointed by the President with the advice and consent of the Senate.

- Section 410 of S. 1538 would create an Inspector General (IG) of the IC in the ODNI. In addition to creating yet another new Senate-confirmed position, this provision would authorize the new IC IG to conduct, supervise, and provide policy direction for investigations in any element of the IC, even though that element may be part of a department or agency that already has a statutory IG. The existing IGs of all the IC elements are still best suited to performing their investigative, inspection, and audit functions, without the addition of an outside entity like the proposed new IG. In addition, section 433 would designate the IGs of the Defense Intelligence Agency (DIA), NGA, and the NRO as IGs of designated Federal agencies under the Inspector General Act and makes these officers designees of the IG of the Department of Defense. It also provides that the DNI or the Secretary of Defense may prohibit any of these officers from initiating, carrying out, or completing any audit or investigation that would harm the national security interests of the United States. Authorizing the DNI to cut off an investigation by a departmental inspector general of an intelligence element of an executive department that has been ordered by the head of that executive department would be inconsistent with the preservation of the authority of heads of departments and agencies over their respective departments, as provided in section 1018 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) (Public Law 108-458).

Other Provisions of Concern

The Administration has additional concerns with certain other provisions of S. 1538 and H.R. 2082.

Both S. 1538 and H.R. 2082

Certain reporting requirements in both bills raise concerns with respect to the President's authority to control access to national security information and potentially frustrate the DNI's statutory responsibility to protect sources and methods. Existing law and understandings provide the proper arrangements for ensuring that appropriate congressional committees are informed of intelligence and intelligence-related activities.

- The Administration strongly opposes section 409 of H.R. 2082, which relates to an intelligence special access program inventory. The Administration has serious security and counterintelligence concerns over the creation of a single document that would describe all special access programs. The IC has provided and intends to continue its practice of providing detailed briefings to the intelligence committees on these matters.

- Similarly, section 309 of S. 1538 would direct the DNI to provide a comprehensive report on compliance with the Detainee Treatment Act of 2005 and related provisions of the Military Commissions Act of 2006. The information required in the reports would be extraordinarily classified and is required to include all legal justifications from any office or Official of the Department of Justice. As such, this provision could not only infringe upon the President's responsibility to control access to national security information, but would compel the production of internal deliberative legal materials.

The Administration strongly opposes any efforts, such as those found in section 105 of both S. 1538 and H.R. 2082, to incorporate into law the reporting requirements which may be contained in the conference report or the classified annex to intelligence bill. This would severely restrict the flexibility of both the Congress and the Executive Branch to modify and adapt provisions in the classified annex to meet changing conditions and requirements without seeking a statutory change. We fear that this will inevitably lead to a body of stagnant, outdated reporting requirements that would not meet Congress' information requirements and would drain limited resources in the IC.

Both section 425 of S. 1538 and section 415 of H.R. 2082 would direct the DNI to prepare a report on the advisability of providing Federal retirement benefits to former employees of Air America and associated companies. The question of whether these individuals are entitled to Federal retirement benefits has been reviewed within the Executive Branch and addressed by the Federal Courts. The Administration is reluctant to divert the limited resources of the ODNI to this issue and requests that this provision be omitted from the conference bill.

S. 1538

The Administration has concerns with section 401 as currently drafted. This section would authorize the DNI to conduct accountability reviews of the elements of the IC and the personnel in those elements, and would provide discretionary authority for the DNI to conduct such reviews if requested by a congressional intelligence committee. The DNI strives to be responsive to requests from Congress, but this process is appropriately left to established channels and should not be subject to detailed statutory requirements.

Section 411 establishes in law the National Counterproliferation Center (NCPC) in the ODNI and creates the IG of the IC as an office in the ODNI. For reasons set forth above, the Administration objects to the creation of the IG of the IC. Although we fully support the existence of the NCPC, we object to its codification in law. This is an unnecessary step, and limits the authority in the IRTPA of the DNI to change the Center if it ceases to meet appropriate intelligence priorities.

Section 412 would establish a National Space Intelligence Office in the ODNI. Although the Administration agrees that space intelligence is an important issue, we do not believe that it requires a dedicated office in the ODNI. The statutory creation of this office infringes on the DNI's authorities and responsibilities to organize and prioritize functions in the IC. Accordingly, we request that this provision not be included in the conference bill.

Section 436 would require the Secretary of Defense to delegate certain authorities to the Director of the National Geospatial-Intelligence Agency concerning the granting of security clearances. This provision is unnecessary and could conflict with the implementation of the Administration's program to reform and improve the security clearance process.

S. 1538 also places many new management reporting requirements on the ODNI and the IC. The ODNI would face difficulty in fulfilling the section 311(c)(9) requirement that the DNI submit, by January 31, "the numerical and percentage increase or decrease of such costs of contractors as compared to the cost of contractors, and the number of contractors, during the prior five fiscal years." Because we are not aware of a completed effort, prior to the ODNI's contractor inventory initiated in June 2006, to comprehensively capture information on the number and costs of contractors throughout the IC, it would be exceedingly difficult for IC agencies and elements to produce this data for the prior five fiscal years. For this reason, should this provision be included in the conference bill, we recommend that the reporting requirement outlined in section 311(c)(9) encompass only the data from fiscal years 2006 and beyond, or that a request for earlier data seek a "best estimate" rather than precise figures. Additionally, the January 31 due date should be amended to align with the release of the President's Budget. We also recommend that section 311 include a definition clarifying that the term "contractor" does not refer to those who build or manufacture commodities for the IC, nor those that provide commercially available services to the IC as defined by Office of Management and Budget Circular A-76.

We also note that the reporting requirements of section 312, regarding a Business Enterprise Architecture, will impose significant new data collection and reporting requirements across the IC. At this time, we do not know the resource impact of this requirement, but because of the relatively low threshold amount contained in the bill, we expect them to be significant.

H.R. 2082

The Administration is disappointed that the House of Representatives did not include provisions in the Administration bill to improve the IC's ability to manage its human capital more effectively and hope to work with Congress to include them.

Section 410, requiring certain reports on the capabilities of Iran and North Korea with respect to the development of nuclear weapons, section 423, requiring certain reports of Central Intelligence Agency (CIA) IG audits of covert actions, section 503, directing the President to submit to Congress a report describing any authorization granted during the previous 10 years to engage in intelligence activities related to the overthrow of a democratically elected government, and section 601, requiring a report concerning best practices about sharing information of terrorist threats, raise concerns with respect to the President's authority to control access to national security information. Existing law and understandings provide the proper arrangements for ensuring that appropriate congressional committees are informed of intelligence and intelligence-related activities.

Section 104 authorizes 1,035 permanent employees and detailees for "the elements within the IC Management Account of the Director of National Intelligence," and limits non-

reimbursable details to a period of less than one year. This restriction was inherited by the ODNI from the defunct Community Management Staff. The Administration has requested that the Congress allow the DNI to enter into agreements for non-reimbursable details of up to three years. We recommend that the conferees adopt section 308 of S. 1538, which conforms to the Administration's proposed language. This would increase the DNI's staffing flexibility and facilitate the rotation of IC employees, especially those on joint duty assignments.

The Administration opposes section 106, which would cap the authorized positions in the ODNI at the number of personnel serving in the Office on May 1, 2007. While we share the concern of controlling the growth of the ODNI, we are also aware of the new requirements on the ODNI. The Administration is concerned that such caps make it difficult to achieve the appropriate mix of staff and contractor employees. Consequently, we believe that it is necessary that the DNI be given flexibility to determine the actual staffing requirements for the Office. Indeed, such caps are completely inconsistent with the numerous new offices, reports, and responsibilities placed on the DNI by these bills.

The Administration opposes section 307, which would prohibit the heads of elements of the IC from implementing any pay-for-performance plan until after the DNI submits a prescribed report to Congress. Section 307 unnecessarily restricts the ability of IC agencies, such as those in the Departments of Defense and Homeland Security, to implement tailored pay plans under other existing statutory authorities. It would also hinder Administration efforts to establish a program within the IC to provide common pay, performance evaluation and benefits throughout the Community. As an alternative to a requirement for a formal report, we suggest that the ODNI continue to provide briefings to Congress on the IC's human capital proposals as they are developed and implemented.

Section 404 would establish the National Counterproliferation Center within the ODNI providing that the Director of the Center shall be appointed by the DNI. As the Center has been established and a head of the Center appointed, the Administration believes that this provision is unnecessary.

The Administration does not support section 406, which would require the DNI to establish multilevel security clearances, for the stated purpose of enabling the IC to make use of persons proficient in foreign languages. Elements of the IC have already established security processing procedures, unique to each agency's requirements for linguists and consistent with the President's duty to protect sensitive national security information. These and other procedures, such as expedited processing, and granting clearances and accesses up to the level actually required for an individual position may address the problem without the need for a new security clearance structure.

Section 407 would require the DNI to submit a National Intelligence Estimate (NIE) on the anticipated security and geopolitical effects of global climate change. Work on this assessment has already begun and this provision is unnecessary.

The Administration is concerned about the reporting requirements in section 411 of H.R. 2082. Although we understand the concern over increased use of contractors by the IC - indeed

we share that concern - we believe that the detailed reporting requirements contained in section 411 could require a considerable amount of IC resources to complete. In the alternative, we would ask the conferees to consider dropping the reporting requirements as currently drafted, and substitute a requirement for periodic briefings to the intelligence committees on the use of contractors in the IC.

Section 412 would require the DNI to provide members and staff of the intelligence committees with an annual report on foreign language proficiency in the IC. ODNI already collects the majority of the information requested by this provision and the Administration does not support a statutory change to the annual reporting requirements of IRTPA. However, should the conferees include this report, we request that implementation be set to coincide with the Fiscal Year 2008 annual report. This change would permit modifications to current and future data collection efforts to compile the requested information.

Section 501 would prohibit the Secretary of Defense from beginning the process of terminating the U-2 aircraft program until he certifies to Congress that there would be no loss of national or DoD intelligence, surveillance, and reconnaissance capabilities in transitioning from the U-2 to the Global Hawk RQ-4 unmanned aerial vehicle platform. This provision duplicates Section 133 of Public Law 109-364, the FY2007 defense authorization act, which has already been implemented. Imposing this duplicative new reporting requirement would serve no useful purpose and would interfere with the orderly execution of the ongoing transition program. The Administration urges the conferees not to include this provision in the final bill.

Provisions to Include in the Conference Bill

The Administration has determined that the following provisions are particularly important to the IC, and we urge the conferees to adopt them in the conference bill. Where appropriate we suggest revisions.

Both S. 1538 and H.R. 2082

Section 406 of S. 1538 and section 401 of H.R. 2082 would amend the section of the IRTPA that prohibits the co-location of the ODNI with any element of the IC after October 1, 2008. This prohibition would prohibit the co-location of the headquarters of the ODNI with the headquarters of any other element of the IC. The Administration supports these provisions; however, they omit a grant of authority to the President to waive the ban on co-location where the cost of providing separate facilities is unwarranted or for reasons of national security. This authority to waive the ban affords flexibility to ensure that the ODNI or its various components may be located in the most appropriate facility or facilities. Because the ODNI handles some of the most sensitive intelligence information within the U.S. Government, it is important that the ODNI have the highest level of physical and technical security possible. Considering the difficulty and cost of finding or building a facility that meets the appropriate physical and technical security standards, the President must have the discretion to locate any or all components of the ODNI in one or more existing IC facilities if doing so would be in the interests of the national security.

Both bills contain similar provisions that increase flexibility and consistency of authorities in the IC. Section 304 of S. 1538 and section 306 of H.R. 2082 authorize delegation of authority for travel on common carriers for intelligence collection personnel pursuant to guidelines issued by the DNI. Section 307 of S. 1538 and section 304 of H.R. 2082 would extend to other elements of the IC an authority currently held by the CIA to delete information concerning foreign gifts from reports to the Secretary of State when the publication of that information could adversely affect intelligence sources and methods. The Administration supports their inclusion in the conference bill.

Finally, both bills contain nearly identical provisions that make clear the status of the Coast Guard and the Drug Enforcement Administration as elements in the IC. The Administration strongly supports the inclusion of these provisions in the conference bill.

S. 1538

The Administration appreciates the inclusion of requested additional administrative authority contained in section 404 for the DNI to use interagency funding to establish national intelligence centers and boards, commissions, councils and committees. The Administration's bill also included language that would have exempted actions of the ODNI from the judicial review provisions of the Administrative Procedure Act. We recommend that the conferees include this section in the conference bill with the addition of the following provision:

> ``(t) DISCRETION.— The provisions of the Administrative Procedure Act shall not apply to the Director of National Intelligence in the performance of the functions, powers, duties, and actions vested by law in the Director of National Intelligence or the Office of the Director of National Intelligence."

The Administration also supports inclusion of section 403 in the conference bill. Section 403 would amend the limitation on delegation by the DNI of the authority to protect intelligence sources and methods from unauthorized disclosure. The Senate's provision would authorize delegation to any Deputy Director of National Intelligence or the Chief Information Officer of the IC. The Administration's proposal, however, would have removed all limitations to delegation parallel to the prior National Security Act provision that had vested the power without restriction in the former Director of Central Intelligence. The Administration recommends that the conferees consider increasing the flexibility of the DNI to protect sources and methods and not constrain the DNI from delegating the authority.

Section 103, which authorizes the DNI, with the approval of the Director of the Office of Management and Budget (OMB), to exceed authorized personnel levels by up to five percent, is supported by the Administration. Although, this provision will provide some relief to the ODNI, we request that Congress consider the elimination of imposed civilian end-strength ceilings on the IC. Such ceilings are inflexible, lead to increased use of contractors to perform necessary IC functions in lieu of staff employees, and severely hinder the IC's civilian joint duty, student employment, and National Intelligence Reserve Corps programs. In addition, in light of the additional staffing requirements imposed by this bill, elimination of the arbitrary personnel ceiling is entirely appropriate.

The Administration also urges the inclusion of the following provisions of S. 1538 in the conference bill:

- Section 308 increases the one-year limit on non-reimbursable details to three years.

- Section 316 cancels certain outdated and duplicative statutory reporting requirements levied on the IC.

- Section 402 was requested by the Administration. It would enhance the DNI's authorities to permit the transfer of funds outside the National Intelligence Program for the development and fielding of systems of common concern for the collection, processing, analysis, exploitation and dissemination of intelligence.

- Section 405 would enhance the authority of the DNI for flexible personnel management among elements of the IC. This provision, requested by the Administration, would support pay modernization and equalization across the IC. It would authorize the DNI to convert and establish new positions in the excepted service and establish the classification and pay ranges for such positions. It would also authorize the DNI special rates of pay for critical positions. The Administration wishes to clarify that non-Title 5 positions similar to the CIA's excepted service would be included in the provisions. The Administration also recommends inserting in the bill language clarifying that Department of Justice components would retain the current authorities provided in 5 U.S.C. 3151. Finally, this section would authorize the DNI, with the concurrence of the head of the department or agency concerned, to extend to any IC element any authority "to adopt compensation authority, performance management authority, and scholarship authority" enjoyed by any other IC element.

- Section 409 would establish a Reserve for Contingencies of the ODNI. Funds in the Reserve are to be available to support emerging needs, to improve program effectiveness, or to increase efficiency.

- The Administration has sought the provision contained at section 413 for several years. This provision exempts specific categories of ODNI files from the search, review, and disclosure provisions of the Freedom of Information Act (FOIA). The exemption parallels and reinforces the statutory operational files FOIA exemptions already granted to other elements of the IC.

- Section 414 repeals authorities originally given to the National Counter-intelligence Executive (ONCIX) when it was an independent entity, but retains ONCIX's critical authority to enter into non-reimbursable details of unrestricted duration.

- Section 415 extends the exemption to the Federal Advisory Committee Act, currently held by the CIA, to those advisory committees established or used by the ODNI.

- Section 417 would grant the ODNI authority to promulgate regulations to claim exemption from certain provisions of the Privacy Act consistent with those held by CIA.

- Section 423 would provide express statutory authority for CIA to provide protective services to the DNI and to such personnel as the DNI may designate. The provision also authorizes protective personnel to detain or arrest individuals who may pose an imminent threat to persons being protected.

- Section 431 would clarify the authority of the NSA to seek reimbursement of training expenses paid by the agency.

- Section 432 would provide express statutory authority for NSA to provide protective services to designated NSA personnel.

- S. 1538 also would make certain necessary technical amendments to the National Security Act of 1947, the IRTPA, the Central Intelligence Agency Act of 1949, and other provisions of Federal law that are supported by the Administration.

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

Thank you for the opportunity to present our views on behalf of the IC. We look forward to working with the Committees to resolve the remaining issues discussed above. Please do not hesitate to call upon us if we may be of additional assistance.

Sincerely,

J.M. McConnell

cc: The Honorable Christopher S. Bond
The Honorable Peter Hoekstra

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 2 4 2007

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

Dear Mr. Chairman:

I look forward to appearing before the Senate Judiciary Committee to discuss the Protect America Act (PAA) and the Foreign Intelligence Surveillance Act (FISA). However, I am concerned that the Committee does not have the appropriate witnesses joining me to ensure a full dialogue with the Committee on this important topic. The Department of Justice's Kenneth L. Wainstein, Assistant Attorney General of the National Security Division, should serve as a co-witness with me at this important hearing tomorrow, September 25th. My staff has been in discussion with your staff over the past week but apparently no agreement has been reached. Moreover, the Senate-confirmed General Counsel of the Office of the Director of National Intelligence, Benjamin A. Powell, should also appear as a witness to ensure a full, detailed discussion occurs at this hearing.

As the Nation's principal intelligence officer, I can and will address the intelligence requirements and capabilities needed regarding FISA. However, I am not a lawyer. It is likely some of the Judiciary Committee Members will ask questions about specific provisions in the Protect America Act (PAA); they will ask about the meaning behind specific words in the PAA in addition to FISA and its legal underpinnings. The Department of Justice is central to all discussions involving modification to this critical statute. Ken Wainstein has appeared with me in each of the FISA Hearings over the past several months and heads the office responsible for preparing and presenting FISA applications to the court. Ben Powell has also appeared with me at these Hearings and has been closely involved with your staff in all of the FISA discussions, and has been closely involved in the preparation of FISA proposals presented to Congress.

Finally, as you know Mr. Chairman, I have been personally criticized by some in the Congress and in the media for being too visible and central in the Congressional debates on FISA. That is not a role I have chosen, but if I am the single witness before the Judiciary Committee, I am being placed in the role as the lead advocate and perhaps even as a partisan-something I am not.

I appreciate your swift consideration of my request. If you have any questions on this matter, please contact me or my Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

J.M. McConnell

cc: The Honorable Arlen Specter

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 17 2007

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

Dear Mr. Chairman:

In your letter of September 11, 2007 you urged the Office of the Director of National Intelligence (ODNI) to issue a public statement "to confirm that the surveillance used to assist in the recent disruption of the German plot was collected pursuant to the Foreign Intelligence Surveillance Act (FISA), before passage of the Protect America Act." On September 12, 2007, we issued the following public statement:

> "During the Senate Committee on Homeland Security and Governmental Affairs hearing on September 10, 2007, I discussed the critical importance to our national security of the Foreign Intelligence Surveillance Act (FISA), and the recent amendments to FISA made by the Protect America Act. The Protect America Act was urgently needed by our intelligence professionals to close critical gaps in our capabilities and permit them to more readily follow terrorist threats, such as the plot uncovered in Germany. However, information contributing to the recent arrests was not collected under authorities provided by the Protect America Act."

We appreciate your continuing support for our nation's intelligence programs and look forward to working with the Committee as it works to make permanent FISA improvements. If you have any questions, please contact the ODNI Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted].

Sincerely,

J. M. McConnell

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 2 4 2007

The Honorable Sheldon Whitehouse
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Senator Whitehouse:

Thank you for your recent letter. We deeply appreciate the time and effort you personally devoted to meeting with me and working to ensure we are able to effectively collect intelligence to protect our Nation while safeguarding the civil liberties of all Americans. We regret any misunderstanding created by the compressed timeframe and our actions.

As you noted, we did discuss a narrow proposal at our meeting on 11 July. Between 11 and 27 July, we met with many Members and staff to brief them on modernization of the Foreign Intelligence Surveillance Act (FISA) and better understand their views of the best way to proceed. While these meetings were proceeding, agencies were also considering narrowed statutory language that would ensure we closed and covered critical intelligence gaps. Our April 2007 proposal was in process for over a year and required clearance from several relevant agencies to ensure that the precise language did not harm our capabilities. As we have discussed, FISA is a very complex statute and a single word change can have major consequences. The narrow proposal of July 27 was the result of extracting relevant portions of our April proposal and adding new language. Although there was only a small amount of new text, the verbiage was significant. This change required experts to examine the impact of such an approach and compressed an interagency clearance process that generally takes many months to a matter of days. In the final weeks of this process, intelligence professionals worked around the clock to answer Member and staff questions, participate in briefings and discussion sessions, and at the same time examine several drafting options.

We do regret the misunderstandings that resulted from the urgency of the situation. We have always sought to work in an atmosphere of trust and cooperation and will continue to do so as this process moves forward. If you have any questions on this matter, please contact my Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

J.M. McConnell

UNCLASSIFIED

HARRY REID
NEVADA

MAJORITY LEADER

United States Senate

WASHINGTON, DC 20510-7012

December 16, 2007

Admiral John M. McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Admiral McConnell:

As you know, the Senate will begin debate on the FISA Amendments Act of 2007 this week. Among the issues the Senate will consider is whether to grant retroactive immunity to telecommunications companies that are alleged to have assisted the government in its warrantless wiretapping program. You recently wrote in the New York Times that immunity is one of the three most critical issues in this bill.

We appreciate that you have provided access to the documents necessary for evaluation of this issue to the Senate Intelligence and Judiciary Committees, as each has in turn considered it. As the debate now moves to the full Senate, I believe it is of critical importance that all Senators who will be called upon to vote on this important question have an opportunity to review these key documents themselves so that they may draw their own conclusions. In my view, each sitting Senator has a constitutional right of access to these documents before voting on this matter.

I strongly urge you to make the documents previously provided to the Intelligence and Judiciary Committee regarding retroactive immunity available in a secure location to any Senator who wishes to review them during the floor debate. I appreciate your cooperation in this matter.

Sincerely,

Harry Reid

HARRY REID
Senate Majority Leader

November 14, 2007

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

Dear Mr. Chairman:

This letter presents the views of the Administration on the proposed substitute amendment you circulated to Title I of the FISA Amendments Act of 2007 (S. 2248), a bill "to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that act, and for other purposes." We have appreciated the willingness of Congress to address the need to modernize FISA permanently and to work with the Administration to do so in a manner that allows the intelligence community to collect the foreign intelligence information necessary to protect the Nation while protecting the civil liberties of Americans. With all respect, however, we strongly oppose the proposed substitute amendment. If the substitute is part of a bill that is presented to the President, we and the President's other senior advisers will recommend that he veto the bill.

In August, Congress took an important step toward modernizing the Foreign Intelligence Surveillance Act of 1978 by enacting the Protect America Act of 2007 (PAA). The Protect America Act has allowed us temporarily to close intelligence gaps by enabling our intelligence professionals to collect, without a court order, foreign intelligence information from targets overseas. The intelligence community has implemented the Protect America Act in a responsible way, subject to extensive congressional oversight, to meet the country's foreign intelligence needs while protecting civil liberties. Unless reauthorized by Congress, however, the authority provided in the Protect America Act will expire in less than three months. In the face of the continued terrorist threats to our Nation, we think it is vital that Congress act to make the core authorities of the Protect America Act permanent. Congressional action to provide protection from private lawsuits against companies that are alleged to have assisted the Government in the aftermath of the September 11th terrorist attacks on America also is critical to ensuring the Government can continue to receive private sector help to protect the Nation.

In late October, the Senate Select Committee on Intelligence introduced a consensus, bipartisan bill (S. 2248) that would establish a firm, long-term foundation for our intelligence community's efforts to target terrorists and other foreign intelligence targets located overseas. While the bill is not perfect, it contains many important provisions, and was developed through a thoughtful process that ensured that the intelligence community retains the core authorities it needs to protect the Nation and that the bill would not adversely impact critical intelligence operations. Importantly, that bill would afford retroactive liability protection to communication service providers that are alleged to have assisted the Government with intelligence activities in the aftermath of September 11th. The Intelligence Committee recognized that "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. The

possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." The committee's measured judgment reflects the principle that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions. The bill was reported favorably out of committee on a 13-2 vote.

We respectfully submit that your substitute amendment to Title I of the Senate Intelligence Committee's bill would upset some important provisions in the Intelligence Committee bill. The substitute also does not adequately address certain provisions in the Intelligence Committee's bill that remain in need of improvement. As a result, we have determined, with all respect to your efforts, that the substitute would not provide the intelligence community with the tools it needs effectively to collect foreign intelligence information vital for the security of the Nation.

I. Limitations on Intelligence Collection and National Security Investigations

The substitute would make several amendments to S. 2248 that would have an adverse impact on our ability to collect effectively the foreign intelligence information necessary to protect the Nation. These amendments include the following:

Prohibits Intelligence and Law Enforcement Officials From Using Valuable Investigative Tools. The substitute contains an amendment to the "exclusive means" provision of FISA that could severely harm our ability to conduct national security investigations. As drafted, the provision would bar the use of national security letters, Title III criminal wiretaps, and other well-established investigative tools to collect information in national security investigations.

Threatens Critical Intelligence Collection Activities. The "exclusive means" provision also could harm the national security by disrupting highly classified intelligence activities. Among other things, ambiguities in critical terms and formulations in the provision—including the term "communications information" (a term that is not defined in FISA) and the introduction of the concept of targeting communications (as opposed to persons)—could lead the statute to bar altogether or to require court approval for overseas intelligence activities that involve merely the incidental collection of United States person information.

Limits Existing Provisions of Law that Protect Communications Service Providers. The portion of the substitute regarding protections to communication service providers under Government certifications contains ambiguities that could jeopardize our ability to secure the assistance of these providers in the future. This could hamper significantly the Government's efforts to obtain necessary foreign intelligence information. As the Senate Intelligence Committee noted in its report on S. 2248, "electronic communications service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies."

Allows for Dangerous Intelligence Gaps During the Pendency of an Appeal. The substitute would delete an important provision in the bipartisan Intelligence Committee bill that would ensure that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA Court. Without that provision, whole categories of surveillances directed outside the United States could be halted before review by the FISA Court of Review.

Limits Dissemination of Foreign Intelligence Information. The substitute would impose significant new restrictions on the use of foreign intelligence information, including information not concerning United States persons, obtained or derived from acquisitions using targeting procedures that the FISA Court later found to be unsatisfactory. By requiring analysts to go back to the databases and pull out the information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas. This requirement also strikes us as at odds with the mandate of the September 11th Commission that the intelligence community should find and link disparate pieces of foreign intelligence information. The requirement also harms privacy interests by requiring analysts to examine information that would otherwise be discarded without being reviewed.

Imposes Court Review of Compliance with Minimization Procedures. The substitute would allow the FISA Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information by targeting individuals reasonably believed to be outside the United States. This could place the FISA Court in a position where it would conduct individualized review of the intelligence community's foreign communications intelligence activities. While conferring such authority on the court is understandable in the context of traditional FISA collection, it is anomalous in this context, where the court's role is in approving generally applicable procedures rather than individual surveillances.

Strikes a Provision Designed to Make the FISA Process More Efficient. The substitute would strike a provision from the bipartisan Senate Intelligence Committee bill that would allow the second highest-ranking FBI official to certify applications for electronic surveillance. Today, the only FBI official who can certify FISA applications is the Director, a restriction that can delay the initiation of surveillance when the Director travels or is otherwise unavailable. It is unclear why this provision from the Intelligence Committee bill, which will enhance the efficiency of the FISA process while ensuring high-level accountability, would be objectionable.

II. Necessary Improvements to S. 2248

The substitute also does not make needed improvements to the Senate Intelligence Committee bill. These include:

Provision Pertaining to Surveillance of United States Persons Abroad. The substitute does not make needed improvements to the Committee bill, which would require for the first time that a court order be obtained to surveil United States persons abroad. In addition to being problematic for policy reasons and imposing burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes, the provision continues to have serious technical problems. As drafted, the provision would not allow for the surveillance, even with a court finding, of certain critical foreign intelligence targets, and would allow emergency surveillance outside the United States for significantly less time than the bipartisan Senate Intelligence Committee bill had authorized for surveillance inside the United States.

Maintains a Sunset Provision. Rather than achieving permanent FISA reform, the substitute maintains a six year sunset provision. Indeed, several members on the Judiciary Committee have indicated that they may propose amendments to the bill that would shorten the sunset, leaving the intelligence community and our private partners subject to an uncertain legal framework for collecting intelligence from overseas targets. Any sunset provision withholds from our intelligence professionals the certainty and permanence they need to conduct foreign intelligence collection to protect Americans from terrorism and other threats to the national security. The intelligence community operates much more effectively when the rules governing our intelligence professionals' ability to track our adversaries are established and are not changing from year to year. Stability of law, we submit, also allows the intelligence community to invest resources appropriately. In our respectful view, a sunset provision is unnecessary and would have an adverse impact on the intelligence community's ability to conduct its mission efficiently and effectively.

Fails to Remedy an Unrealistic Reporting Requirement. The substitute fails to make needed amendments to a reporting requirement in the Senate Intelligence Committee bill that poses serious operational difficulties for the intelligence community. The Intelligence Committee bill contains a requirement that intelligence analysts count "the number of persons located in the United States whose communications were reviewed." This provision would be impossible to implement fully. The provision, in short, places potentially insurmountable burdens on intelligence professionals without meaningfully protecting the privacy of Americans. The intelligence community has provided Congress with a further classified discussion of this issue.

We also are concerned by other serious technical flaws in the substitute that create uncertainty.

The Administration remains prepared to work with Congress towards the passage of a permanent FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting and protecting the constitutional rights of Americans, so that the President can sign such a bill into law. We look forward to working with you and the Members of the Judiciary Committee on these important issues.

Thank you for the opportunity to present our views. The Office of Management and

Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of this letter.

Sincerely,

Michael B. Mukasey
Attorney General

J.M. McConnell
Director of National Intelligence

cc: The Honorable Arlen Specter
Ranking Minority Member
The Honorable John D. Rockefeller
Chairman, Select Committee on Intelligence
The Honorable Christopher S. Bond
Vice Chairman, Select Committee on Intelligence