

OLC PART 2

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

<hr/>		
CITIZENS FOR RESPONSIBILITY)	
AND ETHICS IN WASHINGTON)	
)	
Plaintiff-Appellant)	
)	
v.)	No. 08-5409
)	
UNITED STATES DEPARTMENT OF)	
HOMELAND SECURITY)	
)	
Defendant-Appellee)	
<hr/>		

Settlement Agreement Attachment A

Bates numbers of documents to be released in full, except to the extent they are redacted in accordance with paragraph 2 of the Settlement Agreement:

4-5	1650-1652
16	1655
48-50	1657-1658
1203-1207	1664-1670
1370-1378	1675-1690
1380	1695-1696
1384-1385	1757-1758
1389-1396	1781
1416-1417	1816-1817
1419-1424	1818-1828
1426-1428	1839-1840
1436-1437	1845-1846
1441-1446	1865-1877
1506	1883
1520-1521	1911-1912
1526-1529	1914
1531-1546	1917-1922
1620-1622	1923
1629	1926-1928
1639-1641	

Bates numbers of documents to be released in part, subject to the redactions specified below, and also subject to redactions in accordance with paragraph 2 of the Settlement Agreement:

- 2-3: DHS will continue to withhold the names of individuals discussed in these emails.
- 40-43: DHS will continue to withhold the names of individuals discussed in these emails, and will also withhold the third paragraph from the bottom on each of these pages.
- 61: DHS will continue to withhold two paragraphs of the 9/6/05 email from William Carwile.
- 1415: DHS will continue to withhold the text of the top email on the page.
- 1514-1519: DHS will continue to withhold the text of the 9/5/05 email from Brad Gair on page 1518.
- 1560: DHS will continue to withhold the first sentence in the body of the top email.
- 1703-1748: DHS will continue to withhold the second email that appears on page 1704. In addition to being redacted on page 1704, that email will also be redacted on every other page where it appears.
- 1753-1756: DHS will continue to withhold the first sentence in the body of the email on page 1753. In addition to being redacted on page 1753, that sentence will also be redacted on every other page in which it appears.
- 1771-1773: DHS will continue to withhold the names of individuals discussed in these emails.
- 1804-1805: DHS will continue to withhold the names of individuals discussed in these emails, and will also withhold the third paragraph from the bottom on each of these pages.
- 1905-1906: DHS will continue to withhold the names of individuals discussed in these emails.

Hughes, Richard

From: Abegg, John (McConnell)
Sent: Friday, February 23, 2007 4:10 PM
To: Eisenberg, John
Cc: Livingston, J (Intelligence)
Subject: RE: TSP liability protection

@mccconnell.senate.gov] b6

All looks fine to me. I'm looping in Jack Livingston on this email (with whom I've been discussing this legislation) so we are all on the same page. Let us know what Ben says. Thanks.

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

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Friday, February 23, 2007 3:57 PM
To: Abegg, John (McConnell)
Subject: RE: TSP liability protection

John:

1. To make it easier to certify that (1) or (2) is met, without identifying which, we'd propose:

"if the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, THAT either-- (1) (delete "that") the person did not provide the alleged assistance; or (2) (delete "that") the alleged assistance was intended to protect the United States from a terrorist attack."

2. Add comma after "alleged communications intelligence activities"

3. Insert ", without exception," after "proceeding" in section (d).

4. In the third line of (a), could we go with "any other source of law" instead of "any other provision of law"?

I'm also going to see if Ben Powell has suggestions. But this is what we have.

Thanks very much,

John

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

From: Abegg, John (McConnell) [mailto:
Sent: Friday, February 23, 2007 2:07 PM
To: Eisenberg, John
Subject: TSP liability protection

@mccconnell.senate.gov] b6

Please review the revised language and let me know if you have further thoughts. Thanks much.

Berhanu, Tsedey

From: Livingston, J (Intelligence) [✓] @ssci.senate.gov] 66
Sent: Tuesday, February 27, 2007 5:40 PM
To: Eisenberg, John
Subject: Carrier Liability

John,

It looks like Senator Bond is going to sponsor the carrier liability provision that we were working on with John Abegg last week. John mentioned that DOJ might be preparing fact sheets on the current pending cases, e.g., how many, damages sought, cost of legislation, etc. Could I please get copies of what you come up with?
Thanks.

Jack

Berhanu, Tsedey

From: Livingston, J (Intelligence) b6
Sent: Wednesday, February 28, 2007 8:50 PM
To: Eisenberg, John
Subject: RE: Carriers

This is good. Thanks.

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Wednesday, February 28, 2007 7:15 PM
To: Abegg, John (McConnell); Livingston, J (Intelligence)
Cc: Allen, Michael
Subject: Carriers

John/Jack:

Here is what we have on this. Please do not distribute further. Happy to discuss tomorrow.

Thanks,

John

<<Potential Carrier Liability.wpd>>

Hughes, Richard

From: Eisenberg, John
Sent: Tuesday, March 06, 2007 2:24 PM
To: 'Livingston, J (Intelligence)'
Subject: As discussed

Attachments: Substitution_Draft_3_6_07.doc



Substitution_Draft_3_6_07.doc ...

1 SECTION __. SUBSTITUTION OF THE UNITED STATES IN CERTAIN
2 ACTIONS.

3 (a) APPLICABILITY — This section applies to any action or claim brought in any court against
4 a provider of telecommunications, electronic communication or remote computing service,
5 or its employees, officers, or agents, (hereinafter collectively a “provider”) arising from or
6 relating to the alleged provision of any information (including customer information),
7 assistance or facilities to any federal intelligence agency on or after September 11, 2001.

8 The provisions of this section shall apply to any action or claim that is pending on or after
9 the date of enactment.

10 (b) CERTIFICATION BY THE ATTORNEY GENERAL — As to any action or claim described in
11 subsection (a), the Attorney General shall, upon receiving notice of such action or claim,
12 provide a certification to the court if the provider either (1) did not provide any of the
13 information, assistance or facilities alleged, or (2) provided some or all of the information,
14 assistance or facilities (A) pursuant to a written authorization from the head of a department
15 or a federal intelligence agency indicating that such activities had been approved by the
16 President and that such activities were lawful, and (B) in connection with a communications
17 intelligence program authorized by the President after September 11, 2001, designed to
18 identify, track or intercept the communications of international terrorist organizations in
19 order to detect or prevent terrorist attacks against the United States. The certification may
20 be provided in a manner consistent with the protection of state secrets.

21 (c) SUBSTITUTION OF THE UNITED STATES AS A PARTY — Upon receipt by a court of a
22 certification described in subsection (b), a court shall, notwithstanding any other provision
23 of law and without revealing the substance of the certification and consistent with the

1 military and state secrets privilege, substitute the United States for the provider as party-
2 defendant as to all claims designated by the Attorney General in the certification. Upon
3 substitution, the action or proceeding shall proceed in the same manner as any action
4 against the United States filed pursuant to section 1346(b) of title 28, except that section
5 2680(a) of that title shall not apply. The United States shall have the same defenses,
6 privileges and immunities as a private party under like circumstances, and nothing in this
7 section shall be construed to affect the ability of the United States from asserting, in any
8 action or claim described in subsection (a), any privilege, immunity, or defense, including
9 the military and state secrets privilege, that would otherwise have been available to the
10 United States absent its substitution as party-defendant or had the United States been the
11 named defendant. After the substitution of the United States as a party-defendant, the
12 person or entity for whom the United States was substituted shall be dismissed as to all
13 claims designated by the Attorney General as set forth in the certification, and the court
14 shall enter a final judgment and terminate the action as to such person or entity with respect
15 to such claims.

16 (d) PROCEDURE.— Any action that is the subject of a certification by the Attorney General
17 pursuant to subsection (b) shall be removable without bond at any time before trial by the
18 Attorney General to the district court of the United States for the district and division
19 embracing the place wherein it is pending. Notwithstanding 1447(d) of Title 28, the United
20 States may appeal any order of remand entered by any United States district court in an action or
21 proceeding covered by this section.

22 (e) This section (section ____) constitutes the sole waiver of sovereign immunity with respect to
23 any and all actions described in subsection (a). The total liability of the United States under this

1 section (section ____) shall not exceed ten million dollars in the aggregate, and in any particular
2 action described in subsection (a), the total liability of the United States shall not exceed
3 \$10,000.

4 (f) STATE AND LOCAL ENTITIES — No state or local entity may require a provider to
5 disclose information through discovery or otherwise relating to the provider's alleged
6 provision to any federal intelligence agency of any information, facilities or assistance on or
7 after September 11, 2001.

Berhanu, Tsedey

From: Rice, K (Intelligence) [] b6
Sent: Wednesday, March 07, 2007 6:57 PM
To: Eisenberg, John
Subject: RE: amendment to S.4

[It's] I'm heading out in a few minutes—can you give me a call tomorrow? (FYI: although it's been introduced, the amendment hasn't been called up yet so I don't know if it's actually going to be considered. I think cloture on S.4 will be filed tomorrow.) b6

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Wednesday, March 07, 2007 6:40 PM
To: Rice, K (Intelligence)
Subject: RE: amendment to S.4

Can't find your phone number. We have some concerns but need to think it over more. We wouldn't mind chatting about it.

From: Rice, K (Intelligence) [] b6
Sent: Wednesday, March 07, 2007 3:04 PM
To: Eisenberg, John
Subject: amendment to S.4

If you have any thoughts, let us know. Thanks. Kathleen

(b)(5)
in full

Farris, Bette

From: Bradbury, Steve
Sent: Tuesday, March 13, 2007 2:51 PM
To:
Cc:
Subject: Your request

(b)(3) [scribble]

[scribble]

Following up on your request, below are three paragraphs of information and citations on the topic of the emergency that existed in the fall of 2001, the military actions taken by the U.S. in response, and the continuing threat of attack that existed under those circumstances. I hope this is helpful. Steve

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the two towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States—to kill the President, the Vice President, or Members of Congress. The atrocities of September 11th resulted in nearly 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. These attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda's base of operations in Afghanistan. On September 14, 2001, both Houses of Congress passed a joint resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th, which the President signed on September 18th. AUMF § 2(a). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and in particular recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmb1. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime from power.

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11th "created a state of armed conflict." Military Order, § 1 (a), 66 Fed. Reg. 57,833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO took the unprecedented step, for the first time in its 46-year history, of invoking article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), *available at* <http://www.nato.int/docu/speech/2001/s011002a.htm> ("[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by

Article 5 of the Washington Treaty . . ."). The President also determined in his Military Order that al Qaeda and related terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57,833-34.

Hughes, Richard

From: Roland, Sarah E
Sent: Monday, April 09, 2007 5:53 PM
To: Bradbury, Steve; [redacted]; 'Louis Tucker'
Cc: [redacted]; 'Benjamin Powell'; Wainstein, Kenneth (NSD); Olsen, Matt; Gerry, Brett (NSD); Eisenberg, John; Tracci, Robert N
Subject: RE: Tomorrow's 2:30pm

b2
b3

Louis,
Rob Tracci and I are the leg points of contact on this for DOJ on this issue.
Thanks.

From: Bradbury, Steve
Sent: Monday, April 09, 2007 5:47 PM
To: [redacted]; Louis Tucker
Cc: [redacted]; Benjamin Powell; Wainstein, Kenneth (NSD); Olsen, Matt; Gerry, Brett (NSD); Eisenberg, John; Roland, Sarah E; Tracci, Robert N
Subject: RE: Tomorrow's 2:30pm

b2
b3

Please include Ken Wainstein, Matt Olsen, Brett Gerry, and John Eisenberg of DOJ on this. NSD will be taking the lead for DOJ on the April 17 FISA modernization hearing. Thanks!

From: [redacted] mailto:[redacted]
Sent: Monday, April 09, 2007 5:37 PM
To: Louis Tucker
Cc: [redacted]; Bradbury, Steve; Benjamin Powell
Subject: Re: Tomorrow's 2:30pm

b3
b2

Louis: Yes we are aware an will indeed plan to do that. Thanks.

Kathleen Turner
Director of Legislative Affairs
Office of the Director of National Intelligence

b6

-----"Tucker, L \ (Intelligence\)" [redacted] wrote: -----

b6

b2/b3

To: [redacted]
From: "Tucker, L \ (Intelligence\)" [redacted] <Steve.Bradbury@usdoj.gov>
Date: 04/09/2007 03:23PM
Subject: Tomorrow's 2:30pm

/Steve,

Just to close the loop on tomorrow's mtg regarding the open FISA modernization hearing to follow the next Tuesday: our expectation is that you will be presenting 1. areas that are classified and members need to stay away from 2. your recommendation of sensitive areas that are not necessarily classified but are best left for closed session because discussion in those areas may expose sensitive equities

5/19/2008

47

Beyond that we're free to hear from you on other thoughts on this issue. Thanks,

Louis

(Steve - I don't have any e-mails on file from your leg folks so I'm sending this to you; thanks)

Louis Tucker

Minority Staff Director

Senate Select Committee on Intelligence

[]

b6

Farris, Bette

From: @dni.gov
Sent: Monday, April 09, 2007 5:37 PM
To: Louis Tucker
Cc: [redacted] Bradbury, Steve; Benjamin Powell
Subject: Re: Tomorrow's 2:30pm

~~(b)(2)~~ b2
~~(b)(6)~~

b3

Louis: Yes we are aware and will indeed plan to do that. Thanks.

Kathleen Turner
Director of Legislative Affairs
Office of the Director of National Intelligence

b6 ~~(b)(2)~~

~~(b)(6)~~ b6

-----"Tucker, L \ (Intelligence\)" @SSCI.Senate.Gov> wrote: -----

To: <@dni.gov>, [redacted]
From: "Tucker, L \ (Intelligence\)" [redacted] <Steve.Bradbury@usdoj.gov>
Date: 04/09/2007 03:23PM @SSCI.Senate.Gov> b6
Subject: Tomorrow's 2:30pm

b3 b2
b6

Kathleen/Michael/Steve,

Just to close the loop on tomorrow's mtg regarding the open FISA modernization hearing to follow the next Tuesday: our expectation is that you will be presenting 1. areas that are classified and members need to stay away from 2. your recommendation of sensitive areas that are not necessarily classified but are best left for closed session because discussion in those areas may expose sensitive equities

Beyond that we're free to hear from you on other thoughts on this issue. Thanks,

Louis

(Steve - I don't have any e-mails on file from your leg folks so I'm sending this to you; thanks)

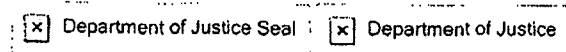
Louis Tucker

Minority Staff Director

Senate Select Committee on Intelligence

b6

~~(b)(6)~~



FOR IMMEDIATE RELEASE
FRIDAY, APRIL 13, 2007
<http://www.usdoj.gov/>

NSD
(202) 514-2007
TDD (202) 514-1888

Fact Sheet: Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act

For over two decades, the Foreign Intelligence Surveillance Act (FISA), as amended, has served as an important framework in the nation's ability to collect foreign intelligence information, while simultaneously protecting the civil liberties of Americans. FISA provides the legal framework through which the Intelligence Community lawfully collects information about those who pose national security threats to our country. FISA helps those in the Intelligence Community catch spies, international terrorists, and others who seek to do harm to the United States, its citizens and its allies.

Today, following over a year of coordinated effort among the Intelligence Community and the Department of Justice a bill is being submitted to Congress to request long overdue changes to FISA. The proposed legislation's core objective is to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the United States.

This legislation is important to ensure that FISA continues to serve the nation as a means to protect our country from foreign security threats, while also continuing to protect the valued privacy interests and civil liberties of persons located in the United States. The Director of National Intelligence, together with the Attorney General, will work with Congress to ensure enactment of this important proposal to keep America safe.

Key Provisions of this Bill Are:

- Updating the definition of electronic surveillance to account for the sweeping changes in telecommunications technology that have taken place.
 - The proposed legislation is technology neutral. In contrast to the 1978 statute, which contains central provisions that are tied to specific communications technologies, this proposal is not tied to specific technology we have today. That way, as telecommunications technology develops over time - - which it surely will do - - FISA will not run the risk of becoming out of date.
- Protecting civil liberties and privacy interests and improving our intelligence capabilities by focusing FISA on people located in the United States.
 - Revolutions in telecommunications technology have brought within FISA's scope communications that Congress did not intend to be covered—and, as a result, extensive resources are now expended obtaining court approval for acquiring communications that do not directly or substantially involve the privacy interests of Americans. Restoring FISA to

its original focus will enhance our intelligence capabilities while allowing the Intelligence Community to devote more resources to protecting the privacy interests of people in the United States.

- Improving the way the United States does business with communications providers.
 - The country's communications providers are important partners in the ability of the United States Government to protect our national security. The proposed legislation includes needed authority both to protect those carriers when they do comply with lawful requests under FISA, and to enable providers to cooperate with authorized intelligence activities.
- Streamlining the FISA process.
 - Numerous Congressional and Executive Branch reviews of the FISA process have recommended that the FISA process be made more efficient, and the Department of Justice has made major strides in recent years in improving its practices and procedures. The proposal would make several changes to improve further the efficiency of the FISA process, including extending the period of authorization for non-United States persons, which will allow the Department and the FISA Court to concentrate more scarce resources to the cases that concern United States persons.
- Reflecting today's national security threats.
 - The Bill seeks to update FISA to reflect today's national security threats. One of those threats is the proliferation of weapons of mass destruction. This legislation will allow the Intelligence Community to obtain FISA authority to better protect the nation against proliferators.
- Adding an additional definition of an agent of a foreign power for non-U.S. persons whom the Government believes possess significant intelligence information, but whose relationship to a foreign power is unclear.
 - This proposed change would apply only to non-United States persons in the United States, and collection of information from such an individual would be subject to the approval of the FISA Court.

###

07-247

Farris, Bette

From: [redacted]
Sent: Thursday, April 19, 2007 12:12 PM
To: Bradbury, Steve
Cc: Eisenberg, John
Subject: RE:

(b)(3) [redacted]

thanks. I look forward to John's email.

[redacted]

[redacted]

(b)(3), (b)(6)

PRIVILEGED ATTORNEY WORK PRODUCT
DO NOT FORWARD

From: Bradbury, Steve [mailto:Steve.Bradbury@usdoj.gov]
Sent: Thursday, April 19, 2007 9:09 AM
To: [redacted]
Cc: Eisenberg, John
Subject: RE:

The DOJ Web site posting is a description of the FISA modernization legislation that the Administration submitted to Congress last week. I believe that bill is public. The third bullet refers to two separate aspects of the legislation. First, the legislation contains a provision that would give carriers immunity from civil liability for assistance they are alleged to have provided the Government since 9/11 in support of the communications intelligence activities of the United States. Second, in connection with the proposed new definition of "electronic surveillance" for FISA purposes, the legislation includes a provision that would enable the Attorney General to compel assistance from carriers in connection with foreign intelligence activities that fall outside the new definition (and for which, therefore, an order of the FISA Court would not be available); this provision would permit carriers to challenge the AG order in court. By copy of this message, I'll ask John Eisenberg to send along to you the relevant provisions from our legislation. I hope that's helpful. Steve

[redacted]

From: [redacted]
Sent: Thursday, April 19, 2007 9:01 AM
To: Bradbury, Steve
Subject:

(b)(3) [redacted]

Steve:

Here is the web reference. See item number 3.

Thanks

5/13/2008

51

[REDACTED]

[REDACTED]

(b) (3), (b) (6)

PRIVILEGED ATTORNEY WORK PRODUCT
DO NOT FORWARD

Farris, Bette

From:

] (b)(3), ~~(b)(7)~~

Sent: Thursday, April 19, 2007 9:01 AM

To: Bradbury, Steve

Attachments: #07-247 04-13-07 Fact Sheet Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act.htm

Steve:

Here is the web reference. See item number 3. *MB*

Thanks

[REDACTED]

(b)(3), (b)(6)

PRIVILEGED ATTORNEY WORK PRODUCT
DO NOT FORWARD

6/23/2008

52

Hughes, Richard

N/A

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

From: Tucker, L (Intelligence)
To: Bradbury, Steve
Sent: Wed May 09 18:36:04 2007
Subject: Re: TSP Document Request

[@SSCI.Senate.Gov]

b6

Steve, your below is correct. Additionally, the other two issues we have not yet discussed and he wants to hear directly from the AG on the reasons for all 3, don't assume it's because he disagrees.

Louis

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

From: Bradbury, Steve <Steve.Bradbury@usdoj.gov>
To: Tucker, L (Intelligence)
Cc: Roland, Sarah E <Sarah.E.Roland@usdoj.gov>
Sent: Wed May 09 18:28:59 2007
Subject: Re: TSP Document Request

Louis: I understood from Vice Chairman Bond's statement at the last hearing that he did not support the Chairman's request that we disclose to the Committee item (2), the DOJ legal opinions. It's one thing to brief the Committee on our legal analysis supporting particular intelligence activities, which we have done; it's another thing entirely to disclose actual deliberative legal advice, in which the Executive Branch has significant and legitimate confidentiality interests. I believe I explained that at the last hearing, and I was convinced that the Vice Chairman recognized and respected that position. Please confirm, if you're able, and I'll discuss these matters with the AG. Thanks. Steve

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

From: Tucker, L (Intelligence)
To: Bradbury, Steve
CC: Roland, Sarah E

[@SSCI.Senate.Gov]

b6

Sent: Wed May 09 18:13:32 2007
Subject: FW: TSP Document Request

Steve,

Let's talk about the below; Bond requests that the AG come by to speak with him soon on this. Thanks,

Louis

From: Livingston, J (Intelligence)
Sent: Wednesday, May 09, 2007 5:24 PM
To: Tucker, L (Intelligence)
Subject: FW: TSP Document Request

Here is what we're waiting on.

From: Healey, C (Intelligence)
Sent: Wednesday, May 09, 2007 4:30 PM
To: Livingston, J (Intelligence); Davidson, M (Intelligence)
Subject: FW: TSP Document Request

Jack -

Mike asked me to get back to you on this. With respect to documents, we are waiting on:

- 1) the President's authorizations of the TSP (as the program evolved);
- 2) the DOJ legal opinions;
- 3) the classified legal pleadings of the government in the various proceedings.

We may also be waiting for answers to various QFRs. I haven't yet checked to see if we received complete answers.

Chris

Hughes, Richard

From: Gerry, Brett (NSD) [redacted] @usdoj.gov
Sent: Thursday, May 31, 2007 9:08 AM
To: [redacted] Davidson, M (Intelligence); Eisenberg, John; [redacted]
Subject: RE: A few minutes before or after this afternoon's FISA discussion

(b)(2)
(b)(6)

After would be slightly preferable for me too, but we could do it either way.

From: [redacted]
Sent: Thursday, May 31, 2007 9:07 AM
To: Davidson, M (Intelligence); Gerry, Brett (NSD); John Eisenberg; [redacted]
Subject: Re: A few minutes before or after this afternoon's FISA discussion

(b)(2)
(b)(6)

Sure, perhaps we could do after FISA meeting.

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

From: "Davidson, M \ (Intelligence\)" [redacted] :sci.senate.gov]
Sent: 05/31/2007 08:48 AM AST
To: Gerry, Brett \ (NSD\)" [redacted] @usdoj.gov>; Eisenberg, John" [redacted] <John.Eisenberg@usdoj.gov>; [redacted]
Subject: A few minutes before or after this afternoon's FISA discussion

(b)(2)
(b)(6)

[redacted] Brett, John, Ben and Kathleen,

(b)(2)
(b)(6)

If you happen to arrive a few minutes before this afternoon's 2 pm FISA discussion, or have a few minutes after, I have a thought and question in relation to next Thursday's hearing here, and about a couple of other June hearing matters.

Mike

Hughes, Richard

From: Eisenberg, John
Sent: Monday, June 11, 2007 6:26 PM
To: 'Bash, Jeremy'; Gerry, Brett (NSD)
Cc: Donesa, Chris; Parker, Wyndee
Subject: RE: Bradbury briefing

Let's play it by ear then, since I don't know what Steve's schedule will be like.

If you have the okay, couldn't the new people be read in by secure phone?

From: Bash, Jeremy ([mailto:jeremy.bash@mail.house.gov])
Sent: Monday, June 11, 2007 6:17 PM
To: Eisenberg, John; Gerry, Brett (NSD)
Cc: Donesa, Chris; Parker, Wyndee
Subject: RE: Bradbury briefing

b6

John,

I expect that new individuals will be read in tomorrow, but not by 1230. Could we push until later in the afternoon or Wednesday? I will have a more refined time tomorrow.

Jeremy

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

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Monday, June 11, 2007 3:40 PM
To: Bash, Jeremy; Gerry, Brett (NSD)
Cc: Donesa, Chris; Parker, Wyndee
Subject: RE: Bradbury briefing

Jeremy:

We can do the Bradbury briefing at 12:30 here tomorrow.

Thanks,

John

From: Bash, Jeremy ([mailto:jeremy.bash@mail.house.gov])
Sent: Monday, June 11, 2007 3:10 PM
To: Gerry, Brett (NSD); Eisenberg, John
Cc: Donesa, Chris; Parker, Wyndee
Subject: Bradbury briefing

b6

I spoke briefly to Brett earlier about the briefing you wanted to give us on the historical development of legal theories for TSP. I told Brett that I don't recall Steve briefing Members on this, but I did find in my notes that Steve briefed staff on June 6, 2006, about this. I was there. So this is a briefing some of us have we've received, but because it's not at all fresh in my mind, it may be useful to do this again. More

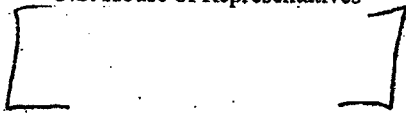
importantly, though, it will be important for the new folks on our staff who are being read into the compartment to get the briefing, as they have not heard it before.

If we can expedite the process of getting those two individuals (Young and Eoyang) read in, we can set the briefing up quickly.

Shall we pencil this in for 12:30 tomorrow for such a briefing? We could do this at DOJ.

JBB

Jeremy Bash | Chief Counsel
Permanent Select Committee on Intelligence
U.S. House of Representatives



b6

Berhanu, Tsedey

From: Livingston, J (Intelligence) [mailto:jlivingst@ssci.senate.gov]
Sent: Friday, July 27, 2007 1:35 PM
To: Kaplan, Joel; Tucker, L (Intelligence); Johnson, K (Intelligence); Rice, K (Intelligence); [mailto:krice@mail.house.gov]; Hawkins, Tom (McConnell); Gerry, Brett (OLP); Olsen, Matthew; Wainstein, Kenneth (NSD); Eisenberg, John; [mailto:jeisenber@mail.house.gov]; Rossi, Nick (Judiciary-Rep); Donesa, Chris
Subject: Vice Chairman Bond's FISA Modernization Proposal
Attachments: EAS07945(FISA Mod Packet 2 Ver 3).xml.pdf; EAS07923(FISA Mod Packet 1 Ver 3).xml.pdf



EAS07945(FISA Mod Packet 2 Ver 3).xml.pdf
EAS07923(FISA Mod Packet 1 Ver 3).xml.pdf

On Wednesday, we presented the Vice Chairman's position on FISA Modernization to Mike Davidson and Chris Healey. I've attached a copy (Mod Packet 2) and would appreciate any comments that you might have on improving the discussion draft. It includes the foreign target, carrier liability, and streamlining provisions. (I would note that we would have to modify the current effective date provision consistent with our discussions today)

We urged them to proceed quickly, but they showed no interest in moving expeditiously and left us with the impression that they would get back to us during recess. They did not provide us with a copy of their plan.

In anticipation that something like this could happen and that Congress might want to move more quickly, I had leg counsel prepare a another package (Mod Packet 1) that contained just the foreign target and carrier liability provisions. I've attached that as well. This might have better success at getting through than the longer package.

In my opinion, we can move just as expeditiously on either of these two packages as we can with Ben's proposal. I think a number of us have significant reservations about Mike's proposal, and I'm at a loss on how it solves the current predicament. As Louis stated, members on both sides of our Committee have expressed a desire to get this out of the FISA Court's jurisdiction. Both of these proposals accomplish that objective.

Thanks.

Jack

110TH CONGRESS
1ST SESSION

S. _____

To amend the Foreign Intelligence Surveillance Act of 1978, to modernize
the provisions of that Act.

IN THE SENATE OF THE UNITED STATES

Mr. BOND introduced the following bill, which was read twice and referred to
the Committee on

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978,
to modernize the provisions of that Act.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Foreign Intelligence Surveillance Modernization Act of
6 2007”.

7 (b) **TABLE OF CONTENTS.**—The table of contents for
8 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Attorney General authorization for acquisition of certain foreign intel-
ligence information.

Sec. 4. Liability defense.

- Sec. 5. Use of information.
- Sec. 6. Applications for court orders.
- Sec. 7. Issuance of an order.
- Sec. 8. Amendments for physical searches.
- Sec. 9. Amendments for emergency pen registers and trap and trace devices.
- Sec. 10. Weapons of mass destruction.
- Sec. 11. Designation of Judges.
- Sec. 12. Technical and conforming amendments.
- Sec. 13. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 (a) **ELECTRONIC SURVEILLANCE.**—Subsection (f) of
3 section 101 of the Foreign Intelligence Surveillance Act
4 of 1978 (50 U.S.C. 1801) is amended to read as follows:

5 “(f) ‘Electronic surveillance’ means—

6 “(1) the installation or use of an electronic, me-
7 chanical, or other surveillance device for acquiring
8 information by intentionally directing surveillance at
9 a particular, known person who is reasonably be-
10 lieved to be located within the United States under
11 circumstances in which that person has a reasonable
12 expectation of privacy and a warrant would be re-
13 quired for law enforcement purposes; or

14 “(2) the intentional acquisition of the contents
15 of any communication under circumstances in which
16 a person has a reasonable expectation of privacy and
17 a warrant would be required for law enforcement
18 purposes, if both the sender and all intended recipi-
19 ents are reasonably believed to be located within the
20 United States.”

1 (b) WIRE COMMUNICATION.—Such section is amend-
2 ed by striking subsection (l).

3 (c) CONTENTS.—Subsection (n) of such section is
4 amended to read as follows:

5 “(n) ‘Contents’, when used with respect to a commu-
6 nication, includes any information concerning the sub-
7 stance, purport, or meaning of that communication.”

8 **SEC. 3. ATTORNEY GENERAL AUTHORIZATION FOR ACQUI-**
9 **SITION OF CERTAIN FOREIGN INTELLIGENCE**
10 **INFORMATION.**

11 (a) IN GENERAL.—The Foreign Intelligence Surveil-
12 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended
13 by inserting the following after section 102:

14 **“AUTHORIZATION FOR ACQUISITION OF CERTAIN**
15 **FOREIGN INTELLIGENCE INFORMATION**

16 **“SEC. 102A. (a) Notwithstanding any other provision**
17 **of law, the President, acting through the Attorney General**
18 **may, for periods of up to 1 year, authorize the acquisition**
19 **of foreign intelligence information concerning persons rea-**
20 **sonably believed to be outside the United States if the At-**
21 **torney General certifies in writing under oath that the At-**
22 **torney General has determined that—**

23 **“(1) the acquisition does not constitute elec-**
24 **tronic surveillance;**

25 **“(2) the acquisition involves obtaining the for-**
26 **eign intelligence information from or with the assist-**

1 ance of a communications service provider, custo-
2 dian, or other person (including any officer, em-
3 ployee, agent, or other specified person of such serv-
4 ice provider, custodian, or other person) who has ac-
5 cess to communications, either as such communica-
6 tions are transmitted or while such communications
7 are stored, or equipment that is being or may be
8 used to transmit or store such communications;

9 “(3) a significant purpose of the acquisition is
10 to obtain foreign intelligence information; and

11 “(4) the minimization procedures to be used
12 with respect to such acquisition activity meet the
13 definition of minimization procedures under section
14 101(h).

15 “(b) A certification under subsection (a) is not re-
16 quired to identify the specific facilities, places, premises,
17 or property at which the acquisition of foreign intelligence
18 information will be directed.

19 “(c) The Attorney General shall immediately trans-
20 mit under seal to the court established under section
21 103(a) a copy of a certification made under subsection (a).
22 Such certification shall be maintained under security
23 measures established by the Chief Justice of the United
24 States and the Attorney General, in consultation with the
25 Director of National Intelligence, and shall remain sealed

1 unless the certification is necessary to determine the legal-
2 ity of the acquisition under section 102B.

3 “(d) An acquisition under this section may be con-
4 ducted only in accordance with the certification of the At-
5 torney General and the minimization procedures adopted
6 by the Attorney General. The Attorney General shall as-
7 sess compliance with such procedures.

8 “DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE
9 AND OTHER ACQUISITIONS OF FOREIGN INTEL-
10 LIGENCE INFORMATION

11 “SEC. 102B. (a) With respect to an authorization of
12 electronic surveillance under section 102 or an authoriza-
13 tion of an acquisition under section 102A, the Attorney
14 General may direct a person to—

15 “(1) immediately provide the Government with
16 all information, facilities, or assistance necessary to
17 accomplish the electronic surveillance or acquisition
18 of foreign intelligence information in such a manner
19 as will protect the secrecy of the electronic surveil-
20 lance or acquisition and produce a minimum of in-
21 terference with the services that such person is pro-
22 viding to the target; and

23 “(2) maintain under security procedures ap-
24 proved by the Attorney General and the Director of
25 National Intelligence any records concerning the

1 electronic surveillance or acquisition or the aid fur-
2 nished that such person wishes to maintain.

3 “(b) The Government shall compensate, at the pre-
4 vailing rate, a person for providing information, facilities,
5 or assistance under subsection (a).

6 “(c) In the case of a failure to comply with a directive
7 issued under subsection (a), the Attorney General may in-
8 voke the aid of the court established under section 103(a)
9 to compel compliance with the directive. The court shall
10 issue an order requiring the person to comply with the
11 directive if it finds that the directive was issued in accord-
12 ance with subsection (a) and is otherwise lawful. Failure
13 to obey an order of the court may be punished by the court
14 as contempt of court. Any process under this section may
15 be served in any judicial district in which the person may
16 be found.

17 “(d)(1)(A) A person receiving a directive issued
18 under subsection (a) may challenge the legality of that di-
19 rective by filing a petition with the pool established under
20 section 103(e)(1).

21 “(B) The presiding judge designated under section
22 103(b) shall assign a petition filed under subparagraph
23 (A) to 1 of the judges serving in the pool established by
24 section 103(e)(1). Not later than 24 hours after the as-
25 signment of such petition, the assigned judge shall conduct

1 an initial review of the directive. If the assigned judge de-
2 termines that the petition is frivolous, the assigned judge
3 shall immediately deny the petition and affirm the direc-
4 tive or any part of the directive that is the subject of the
5 petition. If the assigned judge determines the petition is
6 not frivolous, the assigned judge shall, within 72 hours
7 of the initial review of the directive, consider the petition
8 in accordance with the procedures established under sec-
9 tion 103(e)(2) and provide a written statement for the
10 record of the reasons for any determination under this
11 subsection.

12 “(2) A judge considering a petition under this sub-
13 section to modify or set aside a directive may grant such
14 petition only if the judge finds that such directive does
15 not meet the requirements of this section or is otherwise
16 unlawful. If the judge does not modify or set aside the
17 directive, the judge shall immediately affirm such direc-
18 tive, and order the recipient to comply with such directive.

19 “(3) Any directive not explicitly modified or set aside
20 under this subsection shall remain in full effect.

21 “(e) The Government or a person receiving a directive
22 reviewed under subsection (d) may file a petition with the
23 court of review established under section 103(b) for review
24 of the decision issued under subsection (d) not later than
25 7 days after the issuance of such decision. Such court of

1 review shall have jurisdiction to consider such petitions
2 and shall provide for the record a written statement of
3 the reasons for its decision. On petition for a writ of cer-
4 torari by the Government or any person receiving such
5 directive, the record shall be transmitted under seal to the
6 Supreme Court, which shall have jurisdiction to review
7 such decision.

8 “(f) Judicial proceedings under this section shall be
9 concluded as expeditiously as possible. The record of pro-
10 ceedings, including petitions filed, orders granted, and
11 statements of reasons for decision, shall be maintained
12 under security measures established by the Chief Justice
13 of the United States, in consultation with the Attorney
14 General and the Director of National Intelligence.

15 “(g) All petitions under this section shall be filed
16 under seal. In any proceedings under this section, the
17 court shall, upon request of the Government, review ex
18 parte and in camera any Government submission, or por-
19 tions of a submission, which may include classified infor-
20 mation.

21 “(h) No cause of action shall lie in any court against
22 any person for providing any information, facilities, or as-
23 sistance in accordance with a directive under this section.

24 “(i) A directive made or an order granted under this
25 section shall be retained for a period of not less than 10

1 years from the date on which such directive or such order
2 is made.

3 "USE OF INFORMATION ACQUIRED UNDER SECTION 102A

4 "SEC. 102C. (a) Information acquired from an acqui-
5 sition conducted under section 102A concerning any
6 United States person may be used and disclosed by Fed-
7 eral officers and employees without the consent of the
8 United States person only in accordance with the mini-
9 mization procedures required by section 102A. No other-
10 wise privileged communication obtained in accordance
11 with, or in violation of, the provisions of section 102A shall

12 lose its privileged character. No information from an ac-
13 quisition under section 102A may be used or disclosed by
14 Federal officers or employees except for lawful purposes.

15 "(b) Whenever the Government intends to enter into
16 evidence or otherwise use or disclose in any trial, hearing,
17 or other proceeding in or before any court, department,
18 officer, agency, regulatory body, or other authority of the
19 United States, against a person who was the target of,
20 or whose communications or activities were subject to, an
21 acquisition authorized under section 102A, any informa-
22 tion obtained or derived from such acquisition, the Gov-
23 ernment shall, prior to the trial, hearing, or other pro-
24 ceeding or at a reasonable time prior to an effort to dis-
25 close or so use that information or submit it in evidence,
26 notify such person and the court or other authority in

1 which the information is to be disclosed or used that the
2 Government intends to so disclose or so use such informa-
3 tion.

4 “(c) Whenever any State or political subdivision
5 thereof intends to enter into evidence or otherwise use or
6 disclose in any trial, hearing, or other proceeding in or
7 before any court, department, officer, agency, regulatory
8 body, or other authority of a State or a political subdivi-
9 sion thereof, against a person who was the target of, or
10 whose communications or activities were subject to, an ac-
11 quisition authorized under section 102A, any information
12 obtained or derived from such acquisition, the State or po-
13 litical subdivision thereof shall notify such person, the
14 court, or other authority in which the information is to
15 be disclosed or used, and the Attorney General that the
16 State or political subdivision thereof intends to so disclose
17 or so use such information.

18 “(d)(1) Any person against whom evidence obtained
19 or derived from an acquisition authorized under section
20 102A is to be, or has been, introduced or otherwise used
21 or disclosed in any trial, hearing, or other proceeding in
22 or before any court, department, officer, agency, regu-
23 latory body, or other authority of the United States, a
24 State, or a political subdivision thereof, may move to sup-

1 press the evidence obtained or derived from such acqui-
2 tion on the grounds that—

3 “(A) the information was unlawfully acquired;
4 or

5 “(B) the acquisition was not properly made in
6 conformity with an authorization under section
7 102A.

8 “(2) A person moving to suppress evidence under
9 paragraph (1) shall make such motion before the trial,
10 hearing, or other proceeding unless there was no oppor-
11 tunity to make such a motion or the person was not aware
12 of the grounds of the motion.

13 “(e) Whenever a court or other authority is notified
14 pursuant to subsection (b) or (c) of this section, or when-
15 ever a motion is made pursuant to subsection (d) of this
16 section, or whenever any motion or request is made pursu-
17 ant to any other statute or rule of the United States or
18 any State by a person who was the target of, or whose
19 communications or activities were subject to, an acqui-
20 sition authorized pursuant to section 102A before any court
21 or other authority of the United States or any State—

22 “(1) to discover or obtain applications or orders
23 or other materials relating to an acquisition author-
24 ized pursuant to section 102A; or

1 “(2) to discover, obtain, or suppress evidence or
2 information obtained or derived from an acquisition
3 authorized pursuant to section 102A,
4 the United States district court or, where the motion
5 is made before another authority, the United States
6 district court in the same district as the authority,
7 shall, notwithstanding any other law, if the Attorney
8 General files an affidavit under oath that disclosure
9 or an adversary hearing would harm the national se-
10 curity of the United States, review in camera and ex
11 parte the application, order, and such other mate-
12 rials relating to the acquisition as may be necessary
13 to determine whether such acquisition was lawfully
14 authorized and conducted. In making this deter-
15 mination, the court may disclose to the person who
16 was the target of, or whose communications or ac-
17 tivities were subject to, an acquisition authorized
18 pursuant to section 102A, under appropriate secu-
19 rity procedures and protective orders, portions of the
20 application, order, or other materials relating to the
21 acquisition only where such disclosure is necessary
22 to make an accurate determination of the legality of
23 the acquisition.

24 “(f) If the United States district court, under sub-
25 section (e), determines that an acquisition authorized

1 under section 102A was not lawfully authorized or con-
2 ducted, it shall, in accordance with the requirements of
3 law, suppress the evidence which was unlawfully obtained
4 or derived from the acquisition or otherwise grant the mo-
5 tion of the person who was the target of, or whose commu-
6 nications or activities were subject to, an acquisition au-
7 thorized under section 102A. If the court determines that
8 such acquisition was lawfully authorized and conducted,
9 it shall deny the motion of the person who was the target
10 of, or whose communications or activities were subject to,
11 an acquisition authorized under section 102A except to the
12 extent that due process requires discovery or disclosure.

13 “(g) Orders granting motions or requests under sub-
14 section (f), decisions under this section that an acquisition
15 was not lawfully authorized or conducted, and orders of
16 the United States district court requiring review or grant-
17 ing disclosure of applications, orders, or other materials
18 relating to an acquisition shall be final orders and binding
19 upon all courts of the United States and the several
20 States, except a United States court of appeals and the
21 Supreme Court of the United States.

22 “(h)(1) Federal officers who acquire foreign intel-
23 ligence information under section 102A may consult with
24 Federal law enforcement officers or law enforcement per-
25 sonnel of a State or political subdivision of a State (includ-

1 ing the chief executive officer of that State or political sub-
2 division who has the authority to appoint or direct the
3 chief law enforcement officer of that State or political sub-
4 division) to coordinate efforts to investigate or protect
5 against—

6 “(A) actual or potential attack or other grave
7 hostile acts of a foreign power or an agent of a for-
8 eign power;

9 “(B) sabotage, international terrorism, or the
10 international proliferation of weapons of mass de-
11 struction by a foreign power or an agent of a foreign
12 power; or

13 “(C) clandestine intelligence activities by an in-
14 telligence service or network of a foreign power or by
15 an agent of a foreign power.

16 “(2) Coordination authorized under paragraph (1)
17 shall not preclude the certification required by section
18 102A.

19 “(i) Nothing in this section shall prevent the United
20 States from seeking protective orders or asserting privi-
21 leges ordinarily available to the United States to protect
22 against the disclosure of classified information.”

23 (b) TABLE OF CONTENTS.—The table of contents in
24 the first section of the Foreign Intelligence Surveillance

1 Act of 1978 (50 U.S.C. 1801 et seq.) is amended by in-
2 serting after the item relating to section 102 the following:

“102A. Authorization for acquisition of certain foreign intelligence information.

“102B. Directives relating to electronic surveillance and other acquisitions of
foreign intelligence information.

“102C. Use of information acquired under section 102A.”

3 **SEC. 4. LIABILITY DEFENSE.**

4 (a) **IN GENERAL.**—Notwithstanding any other provi-
5 sion of law, and in addition to the immunities, privileges,
6 and defenses provided by any other source of law, no ac-
7 tion shall lie or be maintained in any court, and no pen-
8 alty, sanction, or other form of remedy or relief shall be
9 imposed by any court or any other body, against any per-
10 son for the alleged provision to an element of the intel-
11 ligence community of any information (including records
12 or other information pertaining to a customer), facilities,
13 or any other form of assistance, during the period begin-
14 ning on September 11, 2001, and ending on the effective
15 date of this Act, in connection with any alleged classified
16 communications intelligence activity that the Attorney
17 General or a designee of the Attorney General certifies,
18 in a manner consistent with the protection of state secrets,
19 is, was, would be, or would have been intended to protect
20 the United States from a terrorist attack. This section
21 shall apply to all actions, claims, or proceedings pending
22 on or after the effective date of this Act.

1 (b) JURISDICTION.—Any action or claim described in
2 subsection (a) that is brought in a State court shall be
3 deemed to arise under the Constitution and laws of the
4 United States and shall be removable under section 1441
5 of title 28, United States Code.

6 (c) DEFINITIONS.—In this section:

7 (1) INTELLIGENCE COMMUNITY.—The term
8 “intelligence community” has the meaning given the
9 term in section 3(4) of the National Security Act of
10 1947 (50 U.S.C. 401a(4)).

11 (2) PERSON.—The term “person” has the
12 meaning given the term in section 2510(6) of title
13 18, United States Code.

14 **SEC. 5. USE OF INFORMATION.**

15 Section 106 of the Foreign Intelligence Surveillance
16 Act of 1978 (50 U.S.C. 1806) is amended—

17 (1) in subsection (i)—

18 (A) by striking “radio communication” and
19 inserting “communication”; and

20 (B) by striking “contents indicates” and
21 inserting “contents contain significant foreign
22 intelligence information or indicate”; and

23 (2) by adding at the end the following:

24 “(l) Nothing in this section shall prevent the United
25 States from seeking protective orders or asserting privi-

1 leges ordinarily available to the United States to protect
2 against the disclosure of classified information.”

3 **SEC. 6. APPLICATIONS FOR COURT ORDERS.**

4 Section 104 of the Foreign Intelligence Surveillance
5 Act of 1978 (50 U.S.C. 1804) is amended—

6 (1) in subsection (a)—

7 (A) by striking paragraphs (2) and (11);

8 (B) by redesignating paragraphs (3)
9 through (10) as paragraphs (2) through (9), re-
10 spectively;

11 (C) in paragraph (5), as redesignated by
12 subparagraph (B) of this paragraph, by striking
13 “detailed”;

14 (D) in paragraph (6), as redesignated by
15 subparagraph (B) of this paragraph, in the
16 matter preceding subparagraph (A)—

17 (i) by striking “Affairs or” and insert-
18 ing “Affairs,”; and

19 (ii) by striking “Senate—” and insert-
20 ing “Senate, or the Deputy Director of the
21 Federal Bureau of Investigation, if des-
22 ignated by the President as a certifying of-
23 ficial—”;

1 (E) in paragraph (7), as redesignated by
2 subparagraph (B) of this paragraph, by striking
3 “statement of” and inserting “listing of”;

4 (F) in paragraph (8), as redesignated by
5 subparagraph (B) of this paragraph, by adding
6 “and” at the end; and

7 (G) in paragraph (9), as redesignated by
8 subparagraph (B) of this paragraph, by striking
9 “; and” and inserting a period;

10 (2) by striking subsection (b);

11 (3) by redesignating subsections (c) through (e)

12 as subsections (b) through (d), respectively; and

13 (4) in paragraph (1)(A) of subsection (d), as re-
14 designated by paragraph (3) of this subsection, by
15 striking “or the Director of National Intelligence”
16 and inserting “the Director of National Intelligence,
17 or the Director of the Central Intelligence Agency”.

18 **SEC. 7. ISSUANCE OF AN ORDER.**

19 Section 105 of the Foreign Intelligence Surveillance
20 Act of 1978 (50 U.S.C. 1805) is amended—

21 (1) in subsection (a)—

22 (A) by striking paragraph (1); and

23 (B) by redesignating paragraphs (2)
24 through (5) as paragraphs (1) through (4), re-
25 spectively;

1 (2) in subsection (c)(1)—

2 (A) in subparagraph (D), by adding “and”
3 at the end;

4 (B) in subparagraph (E), by striking “;
5 and” and inserting a period; and

6 (C) by striking subparagraph (F);

7 (3) by striking subsection (d);

8 (4) by redesignating subsections (e) through (i)
9 as subsections (d) through (h), respectively;

10 (5) in subsection (d), as redesignated by para-
11 graph (4) of this section—

12 (A) in paragraph (1), by striking “120
13 days” and inserting “1 year”; and

14 (B) by amending paragraph (2) to read as
15 follows:

16 “(2) Extensions of an order issued under this title
17 may be granted on the same basis as an original order
18 upon an application for an extension and new findings
19 made in the same manner as required for an original order
20 and may be for a period not to exceed 1 year.”;

21 (6) by amending subsection (e), as redesignated
22 by paragraph (4) of this section, to read as follows:

23 “(e)(1) Notwithstanding any other provision of this
24 title, the Attorney General may authorize the emergency

1 employment of electronic surveillance if the Attorney Gen-
2 eral—

3 “(A) determines that an emergency situation
4 exists with respect to the employment of electronic
5 surveillance to obtain foreign intelligence informa-
6 tion before an order authorizing such surveillance
7 can with due diligence be obtained;

8 “(B) determines that the factual basis for
9 issuance of an order under this title to approve such
10 electronic surveillance exists;

11 “(C) informs a judge having jurisdiction under
12 section 103 at the time of such authorization that
13 the decision has been made to employ emergency
14 electronic surveillance; and

15 “(D) makes an application in accordance with
16 this title to a judge having jurisdiction under section
17 103 as soon as practicable, but not later than 168
18 hours after the Attorney General authorizes such
19 surveillance.

20 “(2) If the Attorney General authorizes the emer-
21 gency employment of electronic surveillance under para-
22 graph (1), the Attorney General shall require that the
23 minimization procedures required by this title for the
24 issuance of a judicial order be followed.

1 “(3) In the absence of a judicial order approving such
2 electronic surveillance, the surveillance shall terminate
3 when the information sought is obtained, when the appli-
4 cation for the order is denied, or after the expiration of
5 168 hours from the time of authorization by the Attorney
6 General, which ever is earliest.

7 “(4) A denial of the application made under this sub-
8 section may be reviewed as provided in section 103.

9 “(5) In the event that such application for approval
10 is denied, or in any other case where the electronic surveil-
11 lance is terminated and no order is issued approving the
12 surveillance, no information obtained or evidence derived
13 from such surveillance shall be received in evidence or oth-
14 erwise disclosed in any trial, hearing, or other proceeding
15 in or before any court, grand jury, department, office,
16 agency, regulatory body, legislative committee, or other
17 authority of the United States, a State, or political sub-
18 division thereof, and no information concerning any
19 United States person acquired from such surveillance shall
20 subsequently be used or disclosed in any other manner by
21 Federal officers or employees without the consent of such
22 person, except with the approval of the Attorney General
23 if the information is significant foreign intelligence infor-
24 mation or indicates a threat of death or serious bodily
25 harm to any person

1 “(6) The Attorney General shall assess compliance
2 with the requirements of paragraph (5).”;

3 (7) in subsection (h), as redesignated by para-
4 graph (4)—

5 (A) by striking “a wire or” and inserting
6 “an”; and

7 (B) by striking “physical search” and in-
8 serting “physical search or in response to a cer-
9 tification by the Attorney General or a designee
10 of the Attorney General seeking information,
11 facilities, or assistance from such person under
12 section 102B”; and

13 (8) by adding at the end the following:

14 “(i) In any case in which the Government makes an
15 application to a judge under this title to conduct electronic
16 surveillance involving communications and the judge
17 grants such application, upon the request of the applicant,
18 the judge shall also authorize the installation and use of
19 pen registers and trap and trace devices, and direct the
20 disclosure of the information set forth in section 402(d)(2)
21 such information shall not be subject to minimization pro-
22 cedures.”.

1 **SEC. 8. AMENDMENTS FOR PHYSICAL SEARCHES.**

2 (a) **APPLICATIONS.**—Section 303 of the Foreign In-
3 telligence Surveillance Act of 1978 (50 U.S.C. 1823) is
4 amended—

5 (1) in subsection (a)—

6 (A) by striking paragraph (2);

7 (B) by redesignating paragraphs (3)
8 through (9) as paragraphs (2) through (8), re-
9 spectively;

10 (C) in paragraph (2), as redesignated by
11 subparagraph (B) of this paragraph, by striking
12 “detailed”;

13 (D) in paragraph (3)(C), as redesignated
14 by subparagraph (B) of this paragraph, by in-
15 serting “or is about to be” before “owned”;

16 (E) in paragraph (6), as redesignated by
17 subparagraph (B) of this paragraph in the mat-
18 ter preceding subparagraph (A)—

19 (i) by striking “Affairs or” and insert-
20 ing “Affairs,”; and

21 (ii) by striking “Senate—” and insert-
22 ing “Senate, or the Deputy Director of the
23 Federal Bureau of Investigation, if des-
24 ignated by the President as a certifying of-
25 ficial—”; and

1 (2) in subsection (d)(1)(A), by striking “or the
2 Director of National Intelligence” and inserting “the
3 Director of National Intelligence, or the Director of
4 the Central Intelligence Agency”.

5 (b) ORDERS.—Section 304 of the Foreign Intel-
6 ligence Surveillance Act of 1978 (50 U.S.C. 1824) is
7 amended—

8 (1) in subsection (a)—

9 (A) by striking paragraph (1);

10 (B) by redesignating paragraphs (2)
11 through (5) as paragraphs (1) through (4), re-
12 spectively; and

13 (C) in paragraph (2)(B), as redesignated
14 by subparagraph (B) of this paragraph, by in-
15 serting “or is about to be” before “owned”;

16 (2) by amending subsection (e) to read as fol-
17 lows:

18 “(e)(1) Notwithstanding any other provision of this
19 title, the Attorney General may authorize the emergency
20 employment of a physical search if the Attorney General—

21 “(A) determines that an emergency situation
22 exists with respect to the employment of a physical
23 search to obtain foreign intelligence information be-
24 fore an order authorizing such physical search can
25 with due diligence be obtained;

1 “(B) determines that the factual basis for
2 issuance of an order under this title to approve such
3 physical search exists;

4 “(C) informs a judge having jurisdiction under
5 section 103 at the time of such authorization that
6 the decision has been made to employ an emergency
7 physical search; and

8 “(D) makes an application in accordance with
9 this title to a judge having jurisdiction under section
10 103 as soon as practicable, but not more than 168
11 hours after the Attorney General authorizes such
12 physical search.

13 “(2) If the Attorney General authorizes the emer-
14 gency employment of a physical search under paragraph
15 (1), the Attorney General shall require that the minimiza-
16 tion procedures required by this title for the issuance of
17 a judicial order be followed.

18 “(3) In the absence of a judicial order approving such
19 physical search, the physical search shall terminate when
20 the information sought is obtained, when the application
21 for the order is denied, or after the expiration of 168
22 hours from the time of authorization by the Attorney Gen-
23 eral, whichever is earliest.

24 “(4) A denial of the application made under this sub-
25 section may be reviewed as provided in section 103.

1 “(5)(A) In the event that such application for ap-
2 proval is denied, or in any other case where the physical
3 search is terminated and no order is issued approving the
4 physical search, no information obtained or evidence de-
5 rived from such physical search shall be received in evi-
6 dence or otherwise disclosed in any trial, hearing, or other
7 proceeding in or before any court, grand jury, department,
8 office, agency, regulatory body, legislative committee, or
9 other authority of the United States, a State, or political
10 subdivision thereof, and no information concerning any
11 United States person acquired from such physical search
12 shall subsequently be used or disclosed in any other man-
13 ner by Federal officers or employees without the consent
14 of such person, except with the approval of the Attorney
15 General if the information is significant foreign intel-
16 ligence information or indicates a threat of death or seri-
17 ous bodily harm to any person.

18 “(B) The Attorney General shall assess compliance
19 with the requirements of subparagraph (A).”

20 (c) CONFORMING AMENDMENTS.—The Foreign Intel-
21 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
22 is amended—

23 (1) in section 304(a)(4), as redesignated by
24 subsection (b) of this section, by striking
25 “303(a)(7)(E)” and inserting “303(a)(6)(E)”; and

1 (2) in section 305(k)(2), by striking
2 “303(a)(7)” and inserting “303(a)(6)”.

3 **SEC. 9. AMENDMENTS FOR EMERGENCY PEN REGISTERS**

4 **AND TRAP AND TRACE DEVICES.**

5 Section 403 of the Foreign Intelligence Surveillance
6 Act of 1978 (50 U.S.C. 1843) is amended—

7 (1) in subsection (a)(2) by striking “48 hours”
8 and inserting “168 hours”; and

9 (2) in subsection (c)(1)(C) by striking “48
10 hours” and inserting “168 hours”.

11 **SEC. 10. WEAPONS OF MASS DESTRUCTION.**

12 (a) **DEFINITIONS.—**

13 (1) **FOREIGN POWER.**—Subsection (a)(4) of sec-
14 tion 101 of the Foreign Intelligence Surveillance Act
15 of 1978 (50 U.S.C. 1801(a)(4)) is amended by in-
16 serting “or the international proliferation of weapons
17 of mass destruction” after “international terrorism”.

18 (2) **AGENT OF A FOREIGN POWER.**—Subsection
19 (b)(1) of such section, as amended by section 2 of
20 this Act, is amended—

21 (A) in subparagraph (C), by striking “or”
22 at the end; and

23 (B) by adding at the end the following:

1 “(E) engages in the international prolifera-
2 tion of weapons of mass destruction, or activi-
3 ties in preparation therefor; or

4 “(F) engages in the international prolifera-
5 tion of weapons of mass destruction, or activi-
6 ties in preparation therefor, for or on behalf of
7 a foreign power; or”

8 (3) FOREIGN INTELLIGENCE INFORMATION.—

9 Subsection (e)(1)(B) of such section is amended by
10 striking “sabotage or international terrorism” and
11 inserting “sabotage, international terrorism, or the
12 international proliferation of weapons of mass de-
13 struction”.

14 (4) TERM.—Such section, as amended by sec-
15 tion 2 of this Act, is amended by inserting after sub-
16 section (o) the following:

17 “(p) ‘Weapon of mass destruction’ means—

18 “(1) any destructive device (as such term is de-
19 fined in section 921 of title 18, United States Code)
20 that is intended or has the capability to cause death
21 or serious bodily injury to a significant number of
22 people;

23 “(2) any weapon that is designed or intended to
24 cause death or serious bodily injury through the re-

1 lease, dissemination, or impact of toxic or poisonous
2 chemicals or their precursors;

3 “(3) any weapon involving a biological agent,
4 toxin, or vector (as those terms are defined in sec-
5 tion 178 of title 18, United States Code); or

6 “(4) any weapon that is designed to release ra-
7 diation or radioactivity at a level dangerous to
8 human life.”.

9 (b) USE OF INFORMATION.—

10 (1) IN GENERAL.—Section 106(k)(1)(B) of the
11 Foreign Intelligence Surveillance Act of 1978 (50
12 U.S.C. 1806(k)(1)(B)) is amended by striking “sab-
13 otage or international terrorism” and inserting “sab-
14 otage, international terrorism, or the international
15 proliferation of weapons of mass destruction”.

16 (2) PHYSICAL SEARCHES.—Section
17 305(k)(1)(B) of such Act (50 U.S.C. 1825(k)(1)(B))
18 is amended by striking “sabotage or international
19 terrorism” and inserting “sabotage, international
20 terrorism, or the international proliferation of weap-
21 ons of mass destruction”.

22 SEC. 11. DESIGNATION OF JUDGES.

23 Section 103 of the Foreign Intelligence Surveillance
24 Act of 1978 (50 U.S.C. 1803) is amended in subsection

1 (a), by inserting “at least” before “seven of the United
2 States judicial circuits”.

3 **SEC. 12. TECHNICAL AND CONFORMING AMENDMENTS.**

4 The Foreign Intelligence Surveillance Act of 1978
5 (50 U.S.C. 1801 et seq.) is amended—

6 (1) in section 103(e)—

7 (A) in paragraph (1), by striking
8 “501(f)(1)” and inserting “102B(d) or
9 501(f)(1)”; and

10 (B) in paragraph (2), by striking
11 “501(f)(1)” and inserting “102B(d) or
12 501(f)(1)”;

13 (2) in section 105—

14 (A) in subsection (a)(4), as redesignated
15 by section 6—

16 (i) by striking “104(a)(7)(E)” and in-
17 serting “104(a)(6)(D)”; and

18 (ii) by striking “104(d)” and inserting
19 “104(c)”;

20 (B) in subsection (e)(1)(A), by striking
21 “104(a)(3)” and inserting “104(a)(2)”;

22 (3) in section 106—

23 (A) in subsection (j), in the matter pre-
24 ceding paragraph (1), by striking “105(e)” and
25 inserting “105(d)”; and

1 (B) in subsection (k)(2), by striking
2 "104(a)(7)(B)" and inserting "104(a)(6)(B)";
3 and

4 (4) in section 108(a)(2)(C), by striking
5 "105(f)" and inserting "105(e)".

6 **SEC. 13. EFFECTIVE DATE.**

7 (a) **IN GENERAL.**—Except as otherwise provided in
8 this Act, the amendments made by this Act shall take ef-
9 fect 90 days after the date of the enactment of this Act.

10 (b) **PENDING ORDERS.**—Notwithstanding any other
11 provision of this Act, any order in effect on the date of
12 enactment of this Act issued under the Foreign Intel-
13 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
14 shall remain in effect until the date of expiration of such
15 order, and, at the request of the applicant, the court estab-
16 lished under section 103(a) of such Act (50 U.S.C.
17 1803(a)) may reauthorize such order if the facts and cir-
18 cumstances continue to justify issuance of such order
19 under the provisions of the Foreign Intelligence Surveil-
20 lance Act of 1978, as in effect on the day before the effec-
21 tive date of this Act. The court established under section
22 103(a) of such Act shall extinguish any such order at the
23 request of the applicant.

110TH CONGRESS
1ST SESSION

S. _____

To amend the Foreign Intelligence Surveillance Act of 1978, to modernize
the provisions of that Act.

IN THE SENATE OF THE UNITED STATES

Mr. BOND introduced the following bill; which was read twice and referred to
the Committee on

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978,
to modernize the provisions of that Act.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Foreign Intelligence Surveillance Modernization Act of
6 2007”.

7 (b) **TABLE OF CONTENTS.**—The table of contents for
8 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Attorney General authorization for acquisition of certain foreign intel-
ligence information.

Sec. 4. Liability defense.

- Sec. 5. Use of information.
Sec. 6. Technical and conforming amendments.
Sec. 7. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 (a) **ELECTRONIC SURVEILLANCE.**—Subsection (f) of
3 section 101 of the Foreign Intelligence Surveillance Act
4 of 1978 (50 U.S.C. 1801) is amended to read as follows:

5 “(f) ‘Electronic surveillance’ means—

6 “(1) the installation or use of an electronic, me-
7 chanical, or other surveillance device for acquiring
8 information by intentionally directing surveillance at
9 a particular, known person who is reasonably be-
10 lieved to be located within the United States under
11 circumstances in which that person has a reasonable
12 expectation of privacy and a warrant would be re-
13 quired for law enforcement purposes; or

14 “(2) the intentional acquisition of the contents
15 of any communication under circumstances in which
16 a person has a reasonable expectation of privacy and
17 a warrant would be required for law enforcement
18 purposes, if both the sender and all intended recipi-
19 ents are reasonably believed to be located within the
20 United States.”

21 (b) **WIRE COMMUNICATION.**—Such section is amend-
22 ed by striking subsection (l).

23 (c) **CONTENTS.**—Subsection (n) of such section is
24 amended to read as follows:

1 “(n) ‘Contents’, when used with respect to a commu-
2 nication, includes any information concerning the sub-
3 stance, purport, or meaning of that communication.”

4 **SEC. 3. ATTORNEY GENERAL AUTHORIZATION FOR ACQUI-**
5 **SITION OF CERTAIN FOREIGN INTELLIGENCE**
6 **INFORMATION.**

7 (a) **IN GENERAL.**—The Foreign Intelligence Surveil-
8 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended
9 by inserting the following after section 102:

10 **“AUTHORIZATION FOR ACQUISITION OF CERTAIN**
11 **FOREIGN INTELLIGENCE INFORMATION**

12 **“SEC. 102A. (a)** Notwithstanding any other provision
13 of law, the President, acting through the Attorney General
14 may, for periods of up to 1 year, authorize the acquisition
15 of foreign intelligence information relating to persons rea-
16 sonably believed to be outside the United States if the At-
17 torney General certifies in writing under oath that the At-
18 torney General has determined that—

19 “(1) the acquisition does not constitute elec-
20 tronic surveillance;

21 “(2) the acquisition involves obtaining the for-
22 eign intelligence information from or with the assist-
23 ance of a communications service provider, custo-
24 dian, or other person (including any officer, em-
25 ployee, agent, or other specified person of such serv-
26 ice provider, custodian, or other person) who has ac-

1 cess to communications, either as such communica-
2 tions are transmitted or while such communications
3 are stored, or equipment that is being or may be
4 used to transmit or store such communications;

5 “(3) a significant purpose of the acquisition is
6 to obtain foreign intelligence information; and

7 “(4) the minimization procedures to be used
8 with respect to such acquisition activity meet the
9 definition of minimization procedures under section
10 101(h).

11 “(b) A certification under subsection (a) is not re-
12 quired to identify the specific facilities, places, premises,
13 or property at which the acquisition of foreign intelligence
14 information will be directed.

15 “(c) The Attorney General shall immediately trans-
16 mit under seal to the court established under section
17 103(a) a copy of a certification made under subsection (a).
18 Such certification shall be maintained under security
19 measures established by the Chief Justice of the United
20 States and the Attorney General, in consultation with the
21 Director of National Intelligence, and shall remain sealed
22 unless the certification is necessary to determine the legal-
23 ity of the acquisition under section 102B.

24 “(d) An acquisition under this section may be con-
25 ducted only in accordance with the applicable certification.

1 of the Attorney General and the minimization procedures
2 adopted by the Attorney General. The Attorney General
3 shall assess compliance with such procedures.

4 "DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE
5 AND OTHER ACQUISITIONS OF FOREIGN INTEL-
6 LIGENCE INFORMATION

7 "SEC. 102B. (a) With respect to an authorization of
8 electronic surveillance under section 102 or an authoriza-
9 tion of an acquisition under section 102A, the Attorney
10 General may direct a person to—

11 "(1) immediately provide the Government with
12 all information, facilities, or assistance necessary to
13 accomplish the electronic surveillance or acquisition
14 of foreign intelligence information in such a manner
15 as will protect the secrecy of the electronic surveil-
16 lance or acquisition and produce a minimum of in-
17 terference with the services that such person is pro-
18 viding to the target; and

19 "(2) maintain under security procedures ap-
20 proved by the Attorney General and the Director of
21 National Intelligence any records relating to the
22 electronic surveillance or acquisition or the aid fur-
23 nished that such person wishes to maintain.

24 "(b) The Government shall compensate, at the pre-
25 vailing rate, a person for providing information, facilities,
26 or assistance under subsection (a).

1 “(c) In the case of a failure to comply with a directive
2 issued under subsection (a), the Attorney General may in-
3 voke the aid of the court established under section 103(a)
4 to compel compliance with the directive. The court shall
5 issue an order requiring the person to comply with the
6 directive if it finds that the directive was issued in accord-
7 ance with subsection (a) and is otherwise lawful. Failure
8 to obey an order of the court under this subsection may
9 be punished by the court as contempt of court. Any proc-
10 ess under this section may be served in any judicial dis-
11 trict in which the person may be found.

12 “(d)(1)(A) A person receiving a directive issued
13 under subsection (a) may challenge the legality of that di-
14 rective by filing a petition with the pool established under
15 section 103(e)(1).

16 “(B) The presiding judge designated under section
17 103(b) shall assign a petition filed under subparagraph
18 (A) to 1 of the judges serving in the pool established by
19 section 103(e)(1). Not later than 24 hours after the as-
20 signment of such petition, the assigned judge shall conduct
21 an initial review of the directive. If the assigned judge de-
22 termines that the petition is frivolous, the assigned judge
23 shall immediately deny the petition and affirm the direc-
24 tive or any part of the directive that is the subject of the
25 petition. If the assigned judge determines the petition is

1 not frivolous, the assigned judge shall, not later than 72
2 hours after the initial review of the directive, consider the
3 petition in accordance with the procedures established
4 under section 103(e)(2) and provide a written statement
5 for the record of the reasons for any determination under
6 this subsection.

7 “(2) A judge considering a petition under this sub-
8 section to modify or set aside a directive may grant such
9 petition only if the judge finds that such directive does
10 not meet the requirements of this section or is otherwise
11 unlawful. If the judge does not modify or set aside the
12 directive, the judge shall immediately affirm such direc-
13 tive, and order the recipient to comply with such directive.

14 “(3) Any directive not explicitly modified or set aside
15 under this subsection shall remain in full effect.

16 “(e) The Government or a person receiving a directive
17 reviewed under subsection (d) may file a petition with the
18 court of review established under section 103(b) for review
19 of the decision issued under subsection (d) not later than
20 7 days after the issuance of such decision. Such court of
21 review shall have jurisdiction to consider such petitions
22 and shall provide for the record a written statement of
23 the reasons for its decision. On petition for a writ of cer-
24 tiorari by the Government or any person receiving such
25 directive, the record shall be transmitted under seal to the

1 Supreme Court of the United States, which shall have ju-
2 risdiction to review such decision.

3 “(f) Judicial proceedings under this section shall be
4 concluded as expeditiously as possible. The record of pro-
5 ceedings, including petitions filed, orders granted, and
6 statements of reasons for decision, shall be maintained
7 under security measures established by the Chief Justice
8 of the United States, in consultation with the Attorney
9 General and the Director of National Intelligence.

10 “(g) All petitions under this section shall be filed
11 under seal. In any proceedings under this section, the
12 court shall, upon request of the Government, review ex
13 parte and in camera any Government submission, or por-
14 tions of a submission, which may include classified infor-
15 mation.

16 “(h) No cause of action shall lie in any court against
17 any person for providing any information, facilities, or as-
18 sistance in accordance with a directive under this section.

19 “(i) A directive made or an order granted under this
20 section shall be retained for a period of not less than 10
21 years from the date on which such directive or such order
22 is made.

23 “USE OF INFORMATION ACQUIRED UNDER SECTION 102A

24 “SEC. 102C. (a) Information acquired from an acqui-
25 sition conducted under section 102A relating to any
26 United States person may be used and disclosed by Fed-

1 eral officers and employees without the consent of the
2 United States person only in accordance with the mini-
3 mization procedures required by section 102A. No other-
4 wise privileged communication obtained in accordance
5 with, or in violation of, the provisions of section 102A shall
6 lose its privileged character. No information from an ac-
7 quisition under section 102A may be used or disclosed by
8 Federal officers or employees except for lawful purposes.

9 “(b) Whenever the Government intends to enter into
10 evidence or otherwise use or disclose in any trial, hearing,
11 or other proceeding in or before any court, department,
12 officer, agency, regulatory body, or other authority of the
13 United States, against a person who was the target of,
14 or whose communications or activities were subject to, an
15 acquisition authorized under section 102A, any informa-
16 tion obtained or derived from such acquisition, the Gov-
17 ernment shall, prior to the trial, hearing, or other pro-
18 ceeding or at a reasonable time prior to an effort to dis-
19 close or so use that information or submit it in evidence,
20 notify such person and the court or other authority in
21 which the information is to be disclosed or used that the
22 Government intends to so disclose or so use such informa-
23 tion.

24 “(c) Whenever any State or political subdivision
25 thereof intends to enter into evidence or otherwise use or

1 disclose in any trial, hearing, or other proceeding in or
2 before any court, department, officer, agency, regulatory
3 body, or other authority of a State or a political subdivi-
4 sion thereof, against a person who was the target of, or
5 whose communications or activities were subject to, an ac-
6 quisition authorized under section 102A, any information
7 obtained or derived from such acquisition, the State or po-
8 litical subdivision thereof shall notify such person, the
9 court, or other authority in which the information is to
10 be disclosed or used, and the Attorney General that the
11 State or political subdivision thereof intends to so disclose
12 or so use such information.

13 “(d)(1) Any person against whom evidence obtained
14 or derived from an acquisition authorized under section
15 102A is to be, or has been, introduced or otherwise used
16 or disclosed in any trial, hearing, or other proceeding in
17 or before any court, department, officer, agency, regu-
18 latory body, or other authority of the United States, a
19 State, or a political subdivision thereof, may move to sup-
20 press the evidence obtained or derived from such acqui-
21 sition on the grounds that—

22 “(A) the information was unlawfully acquired;

23 or

24 “(B) the acquisition was not made in con-
25 formity with an authorization under section 102A.

1 “(2) A person moving to suppress evidence under
2 paragraph (1) shall make such motion before the relevant
3 trial, hearing, or other proceeding, unless there was no
4 opportunity to make such a motion or the person was not
5 aware of the grounds of the motion.

6 “(e) Whenever a court or other authority is notified
7 pursuant to subsection (b) or (c) of this section, or when-
8 ever a motion is made pursuant to subsection (d) of this
9 section, or whenever any motion or request is made pursu-
10 ant to any other statute or rule of the United States or
11 any State by a person who was the target of, or whose
12 communications or activities were subject to, an acquisi-
13 tion authorized pursuant to section 102A before any court
14 or other authority of the United States or any State—

15 “(1) to discover or obtain applications or orders
16 or other materials relating to an acquisition author-
17 ized pursuant to section 102A; or

18 “(2) to discover, obtain, or suppress evidence or
19 information obtained or derived from an acquisition
20 authorized pursuant to section 102A,
21 the United States district court or, where the motion
22 is made before another authority, the United States
23 district court in the same district as the authority,
24 shall, notwithstanding any other law, if the Attorney
25 General files an affidavit under oath that disclosure

1 or an adversary hearing would harm the national se-
2 curity of the United States, review in camera and ex
3 parte the application, order, and such other mate-
4 rials relating to the acquisition as may be necessary
5 to determine whether such acquisition was lawfully
6 authorized and conducted. In making this deter-
7 mination, the court may disclose to the person who
8 was the target of, or whose communications or ac-
9 tivities were subject to, an acquisition authorized
10 pursuant to section 102A, under appropriate secu-
11 rity procedures and protective orders, portions of the
12 application, order, or other materials relating to the
13 acquisition only where such disclosure is necessary
14 to make an accurate determination of the legality of
15 the acquisition.

16 “(f) If a United States district court, under sub-
17 section (e), determines that an acquisition authorized
18 under section 102A was not lawfully authorized or con-
19 ducted, it shall, in accordance with the requirements of
20 law, suppress the evidence which was unlawfully obtained
21 or derived from the acquisition or otherwise grant the mo-
22 tion of the person who was the target of, or whose commu-
23 nications or activities were subject to, an acquisition au-
24 thorized under section 102A. If the court determines that
25 such acquisition was lawfully authorized and conducted,

1 it shall deny the motion of the person who was the target
2 of, or whose communications or activities were subject to,
3 an acquisition authorized under section 102A except to the
4 extent that due process requires discovery or disclosure.

5 “(g) Orders granting motions or requests under sub-
6 section (f), decisions under this section that an acquisition
7 was not lawfully authorized or conducted, and orders of
8 the United States district court requiring review or grant-
9 ing disclosure of applications, orders, or other materials
10 relating to an acquisition shall be final orders and binding
11 upon all courts of the United States and the several
12 States, except a United States court of appeals and the
13 Supreme Court of the United States.

14 “(h)(1) Federal officers who acquire foreign intel-
15 ligence information under section 102A may consult with
16 Federal law enforcement officers or law enforcement per-
17 sonnel of a State or political subdivision of a State (includ-
18 ing the chief executive officer of that State or political sub-
19 division who has the authority to appoint or direct the
20 chief law enforcement officer of that State or political sub-
21 division) to coordinate efforts to investigate or protect
22 against—

23 “(A) actual or potential attack or other grave
24 hostile acts of a foreign power or an agent of a for-
25 eign power;

1 “(B) sabotage or international terrorism; or

2 “(C) clandestine intelligence activities by an in-
3 telligence service or network of a foreign power or by
4 an agent of a foreign power.

5 “(2) Coordination authorized under paragraph (1)
6 shall not preclude the certification required by section
7 102A.

8 “(i) Nothing in this section shall prevent the United
9 States from seeking protective orders or asserting privi-
10 leges ordinarily available to the United States to protect
11 against the disclosure of classified information.”

12 (b) TABLE OF CONTENTS.—The table of contents in
13 the first section of the Foreign Intelligence Surveillance
14 Act of 1978 (50 U.S.C. 1801 et seq.) is amended by in-
15 serting after the item relating to section 102 the following:

“102A. Authorization for acquisition of certain foreign intelligence information.

“102B. Directives relating to electronic surveillance and other acquisitions of
foreign intelligence information.

“102C. Use of information acquired under section 102A.”

16 **SEC. 4. LIABILITY DEFENSE.**

17 (a) IN GENERAL.—Notwithstanding any other provi-
18 sion of law, and in addition to the immunities, privileges,
19 and defenses provided by any other source of law, no ac-
20 tion shall lie or be maintained in any court, and no pen-
21 alty, sanction, or other form of remedy or relief shall be
22 imposed by any court or any other body, against any per-
23 son for the alleged provision to an element of the intel-

1 ligence community of any information (including records
2 or other information pertaining to a customer), facilities,
3 or any other form of assistance, during the period begin-
4 ning on September 11, 2001, and ending on the effective
5 date of this Act, in connection with any alleged classified
6 communications intelligence activity that the Attorney
7 General or a designee of the Attorney General certifies,
8 in a manner consistent with the protection of state secrets,
9 is, was, would be, or would have been intended to protect
10 the United States from a terrorist attack. This section
11 shall apply to all actions, claims, or proceedings pending
12 on or after the effective date of this Act.

13 (b) JURISDICTION.—Any action or claim described in
14 subsection (a) that is brought in a State court shall be
15 deemed to arise under the Constitution and laws of the
16 United States and shall be removable under section 1441
17 of title 28, United States Code.

18 (c) DEFINITIONS.—In this section:

19 (1) INTELLIGENCE COMMUNITY.—The term
20 “intelligence community” has the meaning given the
21 term in section 3(4) of the National Security Act of
22 1947 (50 U.S.C. 401a(4)).

23 (2) PERSON.—The term “person” has the
24 meaning given the term in section 2510(6) of title
25 18, United States Code.

1 **SEC. 5. USE OF INFORMATION.**

2 Section 106 of the Foreign Intelligence Surveillance
3 Act of 1978 (50 U.S.C. 1806) is amended—

4 (1) in subsection (i)—

5 (A) by striking “radio communication” and
6 inserting “communication”; and

7 (B) by striking “contents indicates” and
8 inserting “contents contain significant foreign
9 intelligence information or indicate”; and

10 (2) by adding at the end the following:

11 “(l) Nothing in this section shall prevent the United
12 States from seeking protective orders or asserting privi-
13 leges ordinarily available to the United States to protect
14 against the disclosure of classified information.”

15 **SEC. 6. TECHNICAL AND CONFORMING AMENDMENTS.**

16 Section 103(e) of the Foreign Intelligence Surveil-
17 lance Act of 1978 (50 U.S.C. 1803(e)) is amended—

18 (1) in paragraph (1), by striking “501(f)(1)”
19 and inserting “102B(d) or 501(f)(1)”; and

20 (2) in paragraph (2), by striking “501(f)(1)”
21 and inserting “102B(d) or 501(f)(1)”.

22 **SEC. 7. EFFECTIVE DATE.**

23 (a) **IN GENERAL.**—Except as otherwise provided in
24 this Act, the amendments made by this Act shall take ef-
25 fect 90 days after the date of enactment of this Act.

1 (b) PENDING ORDERS.—Notwithstanding any other
2 provision of this Act, any order in effect on the date of
3 enactment of this Act issued under the Foreign Intel-
4 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)
5 shall remain in effect until the date of expiration of such
6 order, and, at the request of the applicant, the court estab-
7 lished under section 103(a) of such Act (50 U.S.C.
8 1803(a)) may reauthorize such order if the facts and cir-
9 cumstances continue to justify issuance of such order
10 under the provisions of the Foreign Intelligence Surveil-
11 lance Act of 1978, as in effect on the day before the effec-
12 tive date of this Act. The court established under section
13 103(a) of such Act shall extinguish any such order at the
14 request of the applicant.

Berhanu, Tsedey

From: Donesa, Chris [mailto:Chris.Donesa@mail.house.gov]
Sent: Friday, July 27, 2007 9:35 AM
To: 'Potenza, Vito'; Gerry, Brett (OLP); Eisenberg, John; Roland, Sarah E;
Cc: Stewart, Jen
Subject: HPSCI Republican Letter on FISA
Attachments: FISA - Republican Ltr to Chairman 26 Jul 07.pdf

(b)(2)
(b)(6)
(b)(3)

HPSCI Republican Members have sent the attached letter to Chairman Reyes today on the continuing urgent need for FISA modernization.

SILVESTRE REYES, TEXAS, CHAIRMAN

ALCEE L. HASTINGS, FLORIDA, VICE-CHAIRMAN
LEONARD L. ROSSWELL, IOWA
ROBERT E. BUDI-GRAMER, JR., ALABAMA
ARNOLD BISHOP, CALIFORNIA
RICHARD BOLT, NEW JERSEY
CAL DOUGHERTY, MASSACHUSETTS
JOHN F. TIERNEY, MASSACHUSETTS
MIKE THOMPSON, CALIFORNIA
JAMES B. BENTON, ILLINOIS
JAMES R. LANGRISH, RHODE ISLAND
PATRICK J. MURPHY, PENNSYLVANIA

PETER HOEKSTRA, MICHIGAN, RANKING MEMBER
TERRY EVERETT, ALABAMA
HEATHER WILSON, NEW MEXICO
MAC THORNBERRY, TEXAS
JOHN M. McHUGH, NEW YORK
TODD TART, KANSAS
MIKE ROGERS, MICHIGAN
DICK RENZI, ARIZONA
DARRELL E. ISSA, CALIFORNIA

NANCY PELOSI, SPEAKER
JOHN A. BOEHNER, REPUBLICAN LEADER

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

H-405, THE CAPITOL
WASHINGTON, DC 20515
(202) 226-7890

MICHAEL DELANEY
STAFF DIRECTOR
MICHAEL MCHIMANS
MINORITY STAFF DIRECTOR

July 26, 2007

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

Dear Mr. Chairman:

Our country is at enhanced risk of terrorist attack, and the time for dodging and excuses is over. We have long known of the fundamental need to fix the Foreign Intelligence Surveillance Act, and the Committee has been on notice of the urgency of the problem since April 12, when Director McConnell formally transmitted the President's proposal to reform FISA to the Committee. As he further pointed out in a May 21 op-ed in the Washington Post, this legislation would "close critical gaps" and "provide a higher level of protection against terrorist attacks."

Since then, instead of acting with urgency to solve the problem the Committee has held multiple hearings to review years-old disagreements between lawyers about highly specific issues of legal theory that have since been fully and favorably resolved by federal judges. Those issues have no bearing whatsoever on the plain fact that "we are missing a significant portion of what we should be getting" about potential foreign terrorists in foreign countries.

It appears that the majority now is going to walk away from the problem yet again for the August recess while, according to the declassified key judgments of the recent National Intelligence Estimate, Al Qaeda "continues to plan high-impact plots" that are "likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear amongst the US population." We must act immediately and with urgency to close the FISA terrorist loophole and ensure that we are doing everything possible to detect and prevent potential attacks on the American people.

We have seen your letter to Congresswoman Wilson of July 24, and none of the excuses provided justify the Committee's failure to act. We would like to briefly correct

Chairman Reyes
July 26, 2007
Page 2

the record on these issues, and welcome any further discussion you may wish to have on them.

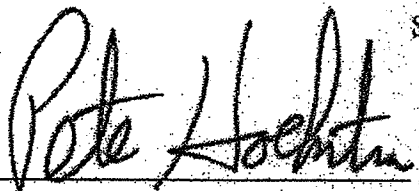
First, you correctly note that FISA has been amended multiple times since the September 11, 2001 attacks. However, this point is completely irrelevant to the fundamental barriers that remain. None of those amendments have in any way changed the fundamentally outdated processes and structures of the law. FISA still contains artificial, decades-old distinctions between wire and radio communications that have not been changed. The urgency of the problem described by Director McConnell and more starkly in our classified briefings obviously still exists regardless of any previous amendments.

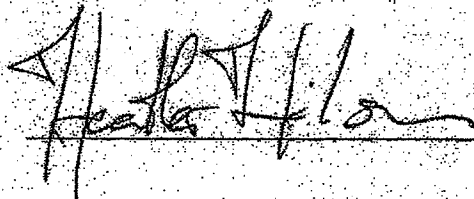
Second, you claim that FISA does not require a court order for communications between foreign targets outside the United States. This does not fully or accurately state the law with respect to FISA, and your position would place intelligence community personnel at potential risk of criminal liability if they were to operate outside of FISA without clear legal authority. Not all of our intelligence is collected under the specific provision of law you mention, and in any event our personnel need clear and binding legal authority in order to obtain cooperation and to have full assurance that their activities are lawful.

Third, you claim that the problem can be easily solved with more lawyers and analysts. Director McConnell told us that that is not the case in his July 26 letter. Moreover, Intelligence Community professionals have told us flatly that that is not the case, and I am surprised that you are politicizing the issue by disregarding their advice. Developing "probable cause" to pass judicial scrutiny is highly specialized, time consuming work requiring specific expertise on overseas terrorist networks. Not only can more of that expertise not be grown overnight, Director McConnell has questioned the wisdom of moving such critical analytic resources from tracking current threats to filling out legal paperwork to protect radical jihadists overseas.

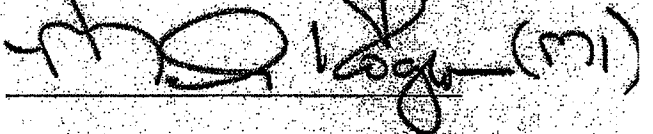
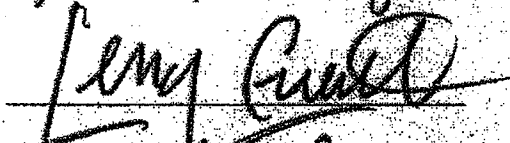
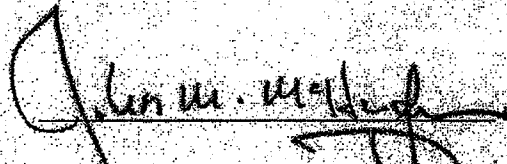
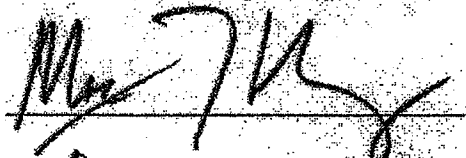
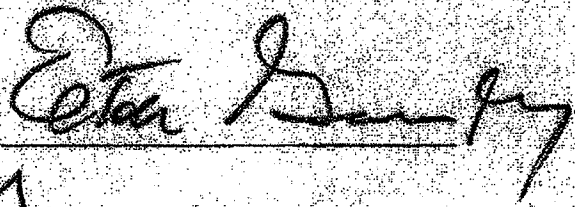
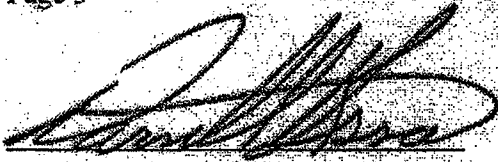
Finally, you claim that the House Intelligence Committee is addressing this issue. We're still waiting while America is at risk of attack.

Sincerely,


Pete Hoekstra


Heather Wilson

Chairman Reyes
July 26, 2007
Page 3



cc: President George W. Bush
Speaker Nancy Pelosi
Republican Leader John Boehner
Majority Leader Steny Hoyer
Majority Whip James Clyburn
Republican Whip Roy Blunt
Members of the House Permanent Select Committee on Intelligence

Farris, Bette

From: Rossi, Nick (Judiciary-Rep) [@judiciary-rep.senate.gov] b6
Sent: Monday, July 30, 2007 6:21 PM
To: Tucker, L (Intelligence); Livingston, J (Intelligence);
Bradbury, Steve; Gerry, Brett (OLP) ~~B~~
Cc: benjamin powell; Rice, K (Intelligence); Roland, Sarah E b2
Subject: Statement Released by Sen. Specter
Attachments: Post Briefing Statement.07302007.doc

I've attached the statement released by Sen. Specter after today's briefing. It conforms to the edits you made to his original draft. I apologize for the difficulty in hammering this out.

Thank you all for the work that went into today's briefing. I think Sen. Specter was persuaded of the need to change FISA to address the concerns highlighted by the DNI.

I am happy to help coordinate a less detailed, but still classified briefing for other Judiciary Committee Members at your earliest convenience.

Regards,
Nick

July 30, 2007

STATEMENT OF SENATOR ARLEN SPECTER

I have received a briefing this afternoon by the Director of National Intelligence and others from the Administration which included matters relating to whether Attorney General Gonzales testified accurately that there was no disagreement in the Administration about the Terrorist Surveillance Program as publicly described by the President. Given the difficulty of discussing classified matters in public, I think it is preferable to have a letter addressing that question from the Administration to Senator Leahy and me by noon tomorrow which will be made available to the news media. The Administration has committed to producing such a letter.

Farris, Bette

From: Rice, K (Intelligence) <@SSCI.senate.gov> (b)(6)
Sent: Monday, July 30, 2007 10:14 AM
To: Tucker, L (Intelligence); Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); Bradbury, Steve; Gerry, Brett (OLP) (b)(2)
Cc: Wolfe, J (Intelligence); Roland, Sarah E
Subject: RE: Mtg with Senator Specter Today at 3 pm

I just reserved 211 Front.

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

From: Tucker, L (Intelligence)
Sent: Monday, July 30, 2007 10:12 AM
To: Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); 'Steve.Bradbury@usdoj.gov'; Wolfe, J (Intelligence); Rice, K (Intelligence); 'Sarah.E.Roland@usdoj.gov'
Subject: Re: Mtg with Senator Specter Today at 3 pm (b)(2)
(b)(6)

Jack and I will both attend, that makes 9 of us so Hart 211 Front would give us more space. Let's plan on that (Wolfe please handle rm skding).

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

From: @dni.gov <@dni.gov>
To: Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); Tucker, L (Intelligence); Steve.Bradbury@usdoj.gov <Steve.Bradbury@usdoj.gov>; Brett Gerry - @usdoj.gov
Cc: Wolfe, J (Intelligence); Benjamin Powell [@dni.gov]; Rice, K (Intelligence); Sarah Roland <Sarah.E.Roland@usdoj.gov>
Sent: Mon Jul 30 10:00:30 2007
Subject: Mtg with Senator Specter Today at 3 pm

The attendees on our side will be:

DNI Mike McConnell
Ben Powell, DNI General Counsel
Steve Bradbury, DoJ
Brett Gerry, DoJ
Kathleen Turner, DNI Leg Affairs

Legislative Branch:

Senator Specter
Nick Rossi
Jack Livingston and/or Louis Tucker

We plan for the DNI to begin with a discussion of the need for FISA Modernization and the current threat backdrop; then move to the evolution of the TSP program and the current FISC opinions.

Would like to do this in hart 219 small conf room.

Many thanks.

Kathleen Turner
Director of Legislative Affairs
Office of the Director of National Intelligence

Farris, Bette

From: Rossi, Nick (Judiciary-Rep) [mailto:rossi@judiciary-rep.senate.gov]
 Sent: Monday, July 30, 2007 3:04 PM
 To: Wolfe, J (Intelligence); Tucker, L (Intelligence); Livingston, J (Intelligence); Bradbury, Steve; Gerry, Brett (OLP)
 Cc: Rice, K (Intelligence); Roland, Sarah E
 Subject: Re: Mtg with Senator Specter Today at 3 pm

(b)(2)
(b)(6)

We are driving back from Union Station. Will be there in just a few minutes. I am told the media may be lurking to get a comment afterwards.

Sent from my BlackBerry Wireless Handheld

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

From: [redacted]
 To: Rossi, Nick (Judiciary-Rep); Wolfe, J (Intelligence); Tucker, L (Intelligence); Livingston, J (Intelligence); Steve Bradbury <Steve.Bradbury@usdoj.gov>; Brett Gerry <brett.gerry@usdoj.gov>; Rice, K (Intelligence); Sarah E Roland <Sarah.E.Roland@usdoj.gov>
 Cc: [redacted]
 Sent: Mon Jul 30 14:51:53 2007
 Subject: Re: Mtg with Senator Specter Today at 3 pm

(b)(2)
(b)(6)

thanks. In car with dni now headed to senate.

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

From: "Rossi, Nick (Judiciary-Rep)" [mailto:rossi@judiciary-rep.senate.gov]
 Sent: 07/30/2007 02:39 PM AST
 To: Wolfe, J (Intelligence)" [mailto:wolfe@ssci.senate.gov]; Tucker, L (Intelligence)" [mailto:tucker@ssci.senate.gov]; kathlpt; Livingston, J (Intelligence)" [mailto:livingston@ssci.senate.gov]; <Steve.Bradbury@usdoj.gov>; <[redacted]@usdoj.gov>
 Cc: [redacted] Rice, K (Intelligence)" [mailto:rice@ssci.senate.gov]; <Sarah.E.Roland@usdoj.gov>
 Subject: Re: Mtg with Senator Specter Today at 3 pm

(b)(2)
(b)(6)

FYI, I am at Union Station to meet Sen. Specter's train. It is apparently running about 10 minutes late, so we may not arrive until a few minutes after 3:00.

Sent from my BlackBerry Wireless Handheld

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

From: Wolfe, J (Intelligence) [mailto:wolfe@ssci.senate.gov]
 To: Tucker, L (Intelligence) [mailto:tucker@ssci.senate.gov]; Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]; [redacted]@usdoj.gov [mailto:[redacted]@usdoj.gov]; [redacted]@usdoj.gov [mailto:[redacted]@usdoj.gov]
 Cc: [redacted] Rice, K (Intelligence); Sarah.E.Roland@usdoj.gov [mailto:Sarah.E.Roland@usdoj.gov]; <[redacted]@usdoj.gov>
 Sent: Mon Jul 30 10:15:11 2007
 Subject: RE: Mtg with Senator Specter Today at 3 pm

(b)(2)
(b)(6)

Done.

James A. Wolfe
Director of Security
U.S. Senate
Select Committee on Intelligence
Washington, D.C. 20510

Direct

(b)(6)

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

From: Tucker, L (Intelligence)
Sent: Monday, July 30, 2007 10:12 AM
To: Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); 'Steve.Bradbury@usdoj.gov'; 'usdoj.gov'
Cc: Wolfe, J (Intelligence); 'Rice, K (Intelligence)'; 'Sarah.E.Roland@usdoj.gov'
Subject: Re: Mtg with Senator Specter Today at 3 pm

(b)(2)
(b)(6)

Jack and I will both attend, that makes 9 of us so Hart 211 Front would give us more space. Let's plan on that (Wolfe please handle rm skding).

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

From: [redacted]
To: Livingston, J (Intelligence); Rossi, Nick (Judiciary-Rep); Tucker, L (Intelligence); Steve.Bradbury@usdoj.gov <Steve.Bradbury@usdoj.gov>; Brett Gerry <Brett.Gerry@usdoj.gov>
Cc: Wolfe, J (Intelligence); Benjamin Powell [redacted]
Rice, K (Intelligence); Sarah Roland <Sarah.E.Roland@usdoj.gov>
Sent: Mon Jul 30 10:00:30 2007
Subject: Mtg with Senator Specter Today at 3 pm

The attendees on our side will be:

DNI Mike McConnell
Ben Powell, DNI General Counsel
Steve Bradbury, DoJ
Brett Gerry, DoJ
Kathleen Turner, DNI Leg Affairs

Legislative Branch:

Senator Specter
Nick Rossi
Jack Livingston and/or Louis Tucker

We plan for the DNI to begin with a discussion of the need for FISA Modernization and the current threat backdrop; then move to the evolution of the TSP program and the current FISC opinions.

Would like to do this in Hart 219 small conf room

Many thanks.

Kathleen Turner
Director of Legislative Affairs
Office of the Director of National Intelligence

b6

(b)(7)

(b)(2)

Berhanu, Tsedey

From: Livingston, J (Intelligence) [] @ssci.senate.gov]
Sent: Monday, July 30, 2007 7:29 PM
To: [] Bradbury, Steve; Gerry, Brett (OLP); []
Olsen, Matthew; Eisenberg, John
Cc: Rice, K (Intelligence)
Subject: FW: Draft
Attachments: HEN07F83_xml.pdf

b2
b3
b6

I just got Mike's latest and greatest. Apparently they made changes to reflect some of the criticism they received during the meeting last week. So much for 12333.

From: Davidson, M (Intelligence)
Sent: Monday, July 30, 2007 7:05 PM
To: Tucker, L (Intelligence); Livingston, J (Intelligence); Rice, K (Intelligence)
Subject: Draft

110TH CONGRESS
1ST SESSION

S. _____

To amend the Foreign Intelligence Surveillance Act of 1978 to establish
a procedure for authorizing certain electronic surveillance.

IN THE SENATE OF THE UNITED STATES

introduced the following bill; which was read twice
and referred to the Committee on

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978
to establish a procedure for authorizing certain electronic
surveillance.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. PURPOSE.**

4 The purpose of this Act is to facilitate the electronic
5 surveillance of persons reasonably believed to be outside
6 the United States in order to obtain foreign intelligence
7 information relating to international terrorism.

1 SEC. 2. ADDITIONAL PROCEDURE FOR AUTHORIZING CER-
2 TAIN ELECTRONIC SURVEILLANCE.

3 (a) IN GENERAL.—The Foreign Intelligence Surveil-
4 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended
5 by inserting after section 105 the following:

6 “ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN
7 ELECTRONIC SURVEILLANCE

8 “SEC. 105A. (a)(1) Notwithstanding any other provi-
9 sion of this title, the Attorney General, upon the author-
10 ization of the President, may apply to a judge of the court
11 established under section 103(a) for an ex parte order, or
12 an extension of an order, authorizing electronic surveil-
13 lance for periods of not more than 1 year, for the purpose
14 of acquiring foreign intelligence information relating to
15 international terrorism, in accordance with this sub-
16 section.

17 “(2)(A) Each application for an order, or extension
18 of an order, submitted under paragraph (1) shall in-
19 clude—

20 “(i) the identity of the Federal officer seeking
21 to conduct such electronic surveillance;

22 “(ii) a description of—

23 “(I) the methods to be used by the Attor-
24 ney General to determine, during the duration
25 of the order, that there is a reasonable belief

1 that the target of the electronic surveillance is
2 a person who is outside the United States; and

3 “(II) the procedures to audit the imple-
4 mentation of the methods described in sub-
5 clause (I) to achieve the objective described in
6 that subclause;

7 “(iii) a description of the nature of the informa-
8 tion sought, including the identity of any foreign
9 power against whom electronic surveillance will be
10 conducted; and

11 “(iv) a statement of the means by which the
12 electronic surveillance will be effected and such other
13 information about the surveillance techniques to be
14 used as may be necessary to assess the proposed
15 minimization procedures.

16 “(B) An application for an order, or extension of an
17 order, submitted under paragraph (1) shall not be re-
18 quired to identify—

19 “(i) the person, other than a foreign power,
20 against whom electronic surveillance will be directed;
21 or

22 “(ii) the specific facilities, places, premises, or
23 property at which the electronic surveillance will be
24 directed.

1 “(3) An application for an order, or extension of an
2 order, submitted under paragraph (1) shall be approved,
3 if the Attorney General certifies in writing under oath, and
4 the judge upon consideration of the application deter-
5 mines, that—

6 “(A) the acquisition does not constitute elec-
7 tronic surveillance within the meaning of paragraph
8 (1) or (3) of section 101(f);

9 “(B) the electronic surveillance is directed at a
10 person reasonably believed to be outside the United
11 States, which may include a foreign power;

12 “(C) the methods described by the Attorney
13 General under paragraph (2)(A)(ii)(I) are reason-
14 ably designed to determine whether the target is a
15 person who is outside the United States;

16 “(D) a significant purpose of the electronic sur-
17 veillance is to obtain foreign intelligence information
18 relating to international terrorism;

19 “(E) the electronic surveillance involves obtain-
20 ing the foreign intelligence information relating to
21 international terrorism from or with the assistance
22 of a communications service provider, custodian, or
23 other person (including any officer, employee, agent,
24 or other specified person of such service provider,
25 custodian, or other person) who has access to the

1 communications that are the subject of the electronic
2 surveillance;

3 “(F) guidelines have been established by the
4 Attorney General to ensure that an application is
5 filed under section 104 to continue electronic surveil-
6 lance against a person outside the United States if
7 there is reason to believe—

8 “(i) that the person is a United States per-
9 son; or

10 “(ii) that a significant number of commu-
11 nications to or from that person involve a per-
12 son who is in the United States; and

13 “(G) the proposed minimization procedures
14 meet the definition of minimization procedures
15 under section 101(h).

16 “(b) The authority under subsection (a) is in addition
17 to the authority to conduct electronic surveillance under
18 sections 104 and 105.

19 “(c) The contents and effect of an order under this
20 section shall be the same as an order under section 105,
21 including that—

22 “(1) if requested by the applicant, a specified
23 communications service provider, custodian, or other
24 specified person, shall furnish the applicant forth-
25 with all information, facilities, or technical assist-

1 ance necessary to accomplish the electronic surveil-
2 lance in such a manner as will protect its secrecy
3 and produce a minimum of interference with the
4 services that provider, custodian, or other person is
5 providing that target of electronic surveillance; and

6 “(2) the liability protections in section 105(i)
7 shall apply to an order under this section.

8 “(d) The court established under section 103(a) shall
9 promptly adopt and, consistent with the protection of na-
10 tional security, publish rules and procedures that set forth
11 the requirements for an application by the Attorney Gen-
12 eral and the proceedings of the court under this section.

13 Except as necessary to carry out the provisions of this sec-
14 tion, the rules shall, to the extent feasible, be consistent
15 with the requirements of sections 104 and 105. The rules
16 and procedures established under this subsection shall be
17 submitted and distributed as provided in section 103(f).

18 “(e) Before issuing an order authorizing electronic
19 surveillance under this section, the judge shall order the
20 applicant to follow the minimization procedures as pro-
21 posed or as modified by the court. The judge may assess
22 compliance with the minimization procedures pursuant to
23 section 105(e)(3) of this title.

24 “(f)(1) Upon the entry of an order under subsection
25 (c), the Attorney General shall submit to the appropriate

1 committees of Congress a report that describes the order
2 and the guidelines established under subsection (a)(3)(F).

3 “(2) The Attorney General shall submit to the appro-
4 priate committees of Congress the results of any audit
5 conducted under the guidelines established under sub-
6 section (a)(3)(F) upon completion of such audit.

7 “(g) Not later than 60 days after the date of enact-
8 ment of this section, and every 60 days thereafter, the At-
9 torney General shall submit to the court established under
10 section 103(a) a report that, for the 60-day period ending
11 on the date of that report, includes—

12 “(1) a list of any target against which elec-
13 tronic surveillance has been directed under this sec-
14 tion;

15 “(2) a list of any target of electronic surveil-
16 lance under this section determined not to have been
17 outside the United States; and

18 “(3) a list of any intelligence report dissemi-
19 nated based on foreign intelligence information ac-
20 quired under this section.

21 “(h) Not later than 60 days after the date of enact-
22 ment of this section, and every 60 days thereafter, the At-
23 torney General shall submit to the appropriate committees
24 of Congress a report that, for the 60-day period ending

1 on the date of that report, includes the information de-
2 scribed in paragraphs (2) and (3) of subsection (g).

3 “(i) Nothing in this section shall be construed to pre-
4 clude the Attorney General from applying for, and a judge
5 from granting, an order under sections 104 and 105 for
6 the electronic surveillance of a person against whom an
7 order may be sought and obtained under those sections.

8 “(j) In this section, the term ‘appropriate committees
9 of Congress’ means—

10 “(1) the Select Committee on Intelligence and
11 the Committee on the Judiciary of the Senate; and

12 “(2) the Permanent Select Committee on Intel-
13 ligence and the Committee on the Judiciary of the
14 House of Representatives.”

15 (b) EFFECTIVE DATE.—The amendments made by
16 this Act shall take effect on the date of enactment of this
17 Act.

18 (c) SUNSET.—

19 (1) IN GENERAL.—Except as provided in para-
20 graph (2), the amendments made by this Act shall
21 cease to have force or effect 180 days after the date
22 of enactment of this Act.

23 (2) EXCEPTION.—Any order under section
24 105A of the Foreign Intelligence Surveillance Act of
25 1978, as added by this Act, in effect on the date de-

1 scribed in paragraph (1) shall continue in effect
2 until the date of the expiration of such order.

3 (d) TECHNICAL AND CONFORMING AMENDMENT.—

4 The table of contents in the first section of the Foreign
5 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et
6 seq.) is amended by inserting after the item relating to
7 section 105 the following:

“Sec. 105A. Additional procedure for authorizing certain electronic surveil-
lance.”

Farris, Bette

From: Livingston, J (Intelligence) [mailto:jlivingston@ssci.senate.gov] b6
Sent: Wednesday, August 01, 2007 10:32 AM
To: Bradbury, Steve; Gerry, Brett (OLP)
Subject: FW: Improvements for EAS07923

Attachments: EAS07962_xml.pdf



EAS07962_xml.pdf
(55 KB)

You all might find portions of this draft helpful as you perfect your current proposal. It's been leg counseled for organization, etc. Sections 7 and 8 may be of use.

110TH CONGRESS
1ST SESSION

S. _____

To amend the Foreign Intelligence Surveillance Act of 1978, to modernize
the provisions of that Act.

IN THE SENATE OF THE UNITED STATES

Mr. BOND introduced the following bill; which was read twice and referred to
the Committee on

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978,
to modernize the provisions of that Act.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Foreign Intelligence Surveillance Modernization Act of
6 2007”.

7 (b) **TABLE OF CONTENTS.**—The table of contents for
8 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Attorney General authorization for acquisition of certain foreign intel-
ligence information.

Sec. 4. Liability defense.

- Sec. 5. Use of information.
Sec. 6. Technical and conforming amendments.
Sec. 7. Construction; severability.
Sec. 8. Effective date; transition procedures; sunset.

1 **SEC. 2. DEFINITIONS.**

2 (a) **ELECTRONIC SURVEILLANCE.**—Subsection (f) of
3 section 101 of the Foreign Intelligence Surveillance Act
4 of 1978 (50 U.S.C. 1801) is amended to read as follows:

5 “(f) ‘Electronic surveillance’ means—

6 “(1) the installation or use of an electronic, me-
7 chanical, or other surveillance device for acquiring
8 information by intentionally directing surveillance at
9 a particular, known person who is reasonably be-
10 lieved to be located within the United States under
11 circumstances in which that person has a reasonable
12 expectation of privacy and a warrant would be re-
13 quired for law enforcement purposes; or

14 “(2) the intentional acquisition of the contents
15 of any communication under circumstances in which
16 a person has a reasonable expectation of privacy and
17 a warrant would be required for law enforcement
18 purposes, if both the sender and all intended recipi-
19 ents are reasonably believed to be located within the
20 United States.”

21 (b) **WIRE COMMUNICATION.**—Such section is amend-
22 ed by striking subsection (l).

1 (c) CONTENTS.—Subsection (n) of such section is
2 amended to read as follows:

3 “(n) ‘Contents’, when used with respect to a commu-
4 nication, includes any information concerning the sub-
5 stance, purport, or meaning of that communication.”.

6 **SEC. 3. ATTORNEY GENERAL AUTHORIZATION FOR ACQUI-**
7 **SITION OF CERTAIN FOREIGN INTELLIGENCE**
8 **INFORMATION.**

9 (a) IN GENERAL.—The Foreign Intelligence Surveil-
10 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended
11 by inserting the following after section 102:

12 “AUTHORIZATION FOR ACQUISITION OF CERTAIN
13 FOREIGN INTELLIGENCE INFORMATION

14 “SEC. 102A. (a) Notwithstanding any other provision
15 of law, the President, acting through the Attorney General
16 may, for periods of up to 1 year, authorize the acquisition
17 of foreign intelligence information relating to persons rea-
18 sonably believed to be outside the United States if the At-
19 torney General certifies in writing under oath that the At-
20 torney General has determined that—

21 “(1) the acquisition does not constitute elec-
22 tronic surveillance;

23 “(2) the acquisition involves obtaining the for-
24 eign intelligence information from or with the assist-
25 ance of a communications service provider, custo-
26 dian, or other person (including any officer, em-

1 employee, agent, or other specified person of such serv-
2 ice provider, custodian, or other person) who has ac-
3 cess to communications, either as such communica-
4 tions are transmitted or while such communications
5 are stored, or equipment that is being or may be
6 used to transmit or store such communications;

7 “(3) a significant purpose of the acquisition is
8 to obtain foreign intelligence information; and

9 “(4) the minimization procedures to be used
10 with respect to such acquisition activity meet the
11 definition of minimization procedures under section
12 101(h).

13 “(b) A certification under subsection (a) is not re-
14 quired to identify the specific facilities, places, premises,
15 or property at which the acquisition of foreign intelligence
16 information will be directed.

17 “(c) The Attorney General shall immediately trans-
18 mit under seal to the court established under section
19 103(a) a copy of a certification made under subsection (a).
20 Such certification shall be maintained under security
21 measures established by the Chief Justice of the United
22 States and the Attorney General, in consultation with the
23 Director of National Intelligence, and shall remain sealed
24 unless the certification is necessary to determine the legal-
25 ity of the acquisition under section 102B.

1 “(d) An acquisition under this section may be con-
2 ducted only in accordance with the applicable certification
3 of the Attorney General and the minimization procedures
4 adopted by the Attorney General. The Attorney General
5 shall assess compliance with such procedures.

6 “DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE
7 AND OTHER ACQUISITIONS OF FOREIGN INTEL-
8 LIGENCE INFORMATION

9 “SEC. 102B. (a) With respect to an authorization of
10 electronic surveillance under section 102 or an authoriza-
11 tion of an acquisition under section 102A, the Attorney
12 General may direct a person to—

13 “(1) immediately provide the Government with
14 all information, facilities, or assistance necessary to
15 accomplish the electronic surveillance or acquisition
16 of foreign intelligence information in such a manner
17 as will protect the secrecy of the electronic surveil-
18 lance or acquisition and produce a minimum of in-
19 terference with the services that such person is pro-
20 viding to the target; and

21 “(2) maintain under security procedures ap-
22 proved by the Attorney General and the Director of
23 National Intelligence any records relating to the
24 electronic surveillance or acquisition or the aid fur-
25 nished that such person wishes to maintain.

1 “(b) The Government shall compensate, at the pre-
2 vailing rate, a person for providing information, facilities,
3 or assistance under subsection (a).

4 “(c) In the case of a failure to comply with a directive
5 issued under subsection (a), the Attorney General may in-
6 voke the aid of the court established under section 103(a)
7 to compel compliance with the directive. The court shall
8 issue an order requiring the person to comply with the
9 directive if it finds that the directive was issued in accord-
10 ance with subsection (a) and is otherwise lawful. Failure
11 to obey an order of the court under this subsection may
12 be punished by the court as contempt of court. Any proc-
13 ess under this section may be served in any judicial dis-
14 trict in which the person may be found.

15 “(d)(1)(A) A person receiving a directive issued
16 under subsection (a) may challenge the legality of that di-
17 rective by filing a petition with the pool established under
18 section 103(e)(1).

19 “(B) The presiding judge designated under section
20 103(b) shall assign a petition filed under subparagraph
21 (A) to 1 of the judges serving in the pool established by
22 section 103(e)(1). Not later than 24 hours after the as-
23 signment of such petition, the assigned judge shall conduct
24 an initial review of the directive. If the assigned judge de-
25 termines that the petition is frivolous, the assigned judge

1 shall immediately deny the petition and affirm the direc-
2 tive or any part of the directive that is the subject of the
3 petition. If the assigned judge determines the petition is
4 not frivolous, the assigned judge shall, not later than 72
5 hours after the initial review of the directive, consider the
6 petition in accordance with the procedures established
7 under section 103(e)(2) and provide a written statement
8 for the record of the reasons for any determination under
9 this subsection.

10 “(2) A judge considering a petition under this sub-
11 section to modify or set aside a directive may grant such
12 petition only if the judge finds that such directive does
13 not meet the requirements of this section or is otherwise
14 unlawful. If the judge does not modify or set aside the
15 directive, the judge shall immediately affirm such direc-
16 tive, and order the recipient to comply with such directive.

17 “(3) Any directive not explicitly modified or set aside
18 under this subsection shall remain in full effect.

19 “(e) The Government or a person receiving a directive
20 reviewed under subsection (d) may file a petition with the
21 court of review established under section 103(b) for review
22 of the decision issued under subsection (d) not later than
23 7 days after the issuance of such decision. Such court of
24 review shall have jurisdiction to consider such petitions
25 and shall provide for the record a written statement of

1 the reasons for its decision. On petition for a writ of cer-
2 tiorari by the Government or any person receiving such
3 directive, the record shall be transmitted under seal to the
4 Supreme Court of the United States, which shall have ju-
5 risdiction to review such decision.

6 “(f) Judicial proceedings under this section shall be
7 concluded as expeditiously as possible. The record of pro-
8 ceedings, including petitions filed, orders granted, and
9 statements of reasons for decision, shall be maintained
10 under security measures established by the Chief Justice
11 of the United States, in consultation with the Attorney
12 General and the Director of National Intelligence.

13 “(g) All petitions under this section shall be filed
14 under seal. In any proceedings under this section, the
15 court shall, upon request of the Government, review ex
16 parte and in camera any Government submission, or por-
17 tions of a submission, which may include classified infor-
18 mation.

19 “(h) No cause of action shall lie in any court against
20 any person for providing any information, facilities, or as-
21 sistance in accordance with a directive under this section.

22 “(i) A directive made or an order granted under this
23 section shall be retained for a period of not less than 10
24 years from the date on which such directive or such order
25 is made.

1 "USE OF INFORMATION ACQUIRED UNDER SECTION 102A

2 "SEC. 102C. (a) Information acquired from an acqui-
3 sition conducted under section 102A relating to any
4 United States person may be used and disclosed by Fed-
5 eral officers and employees without the consent of the
6 United States person only in accordance with the mini-
7 mization procedures required by section 102A. No other-
8 wise privileged communication obtained in accordance
9 with, or in violation of, the provisions of section 102A shall
10 lose its privileged character. No information from an ac-
11 quisition under section 102A may be used or disclosed by
12 Federal officers or employees except for lawful purposes.

13 "(b) Whenever the Government intends to enter into
14 evidence or otherwise use or disclose in any trial, hearing,
15 or other proceeding in or before any court, department,
16 officer, agency, regulatory body, or other authority of the
17 United States, against a person who was the target of,
18 or whose communications or activities were subject to, an
19 acquisition authorized under section 102A, any informa-
20 tion obtained or derived from such acquisition, the Gov-
21 ernment shall, prior to the trial, hearing, or other pro-
22 ceeding or at a reasonable time prior to an effort to dis-
23 close or so use that information or submit it in evidence,
24 notify such person and the court or other authority in
25 which the information is to be disclosed or used that the

1 Government intends to so disclose or so use such informa-
2 tion.

3 “(c) Whenever any State or political subdivision
4 thereof intends to enter into evidence or otherwise use or
5 disclose in any trial, hearing, or other proceeding in or
6 before any court, department, officer, agency, regulatory
7 body, or other authority of a State or a political subdivi-
8 sion thereof, against a person who was the target of, or
9 whose communications or activities were subject to, an ac-
10 quisition authorized under section 102A, any information
11 obtained or derived from such acquisition, the State or po-
12 litical subdivision thereof shall notify such person, the
13 court, or other authority in which the information is to
14 be disclosed or used, and the Attorney General that the
15 State or political subdivision thereof intends to so disclose
16 or so use such information.

17 “(d)(1) Any person against whom evidence obtained
18 or derived from an acquisition authorized under section
19 102A is to be, or has been, introduced or otherwise used
20 or disclosed in any trial, hearing, or other proceeding in
21 or before any court, department, officer, agency, regu-
22 latory body, or other authority of the United States, a
23 State, or a political subdivision thereof, may move to sup-
24 press the evidence obtained or derived from such acqui-
25 sion on the grounds that—

1 “(A) the information was unlawfully acquired;
2 or

3 “(B) the acquisition was not made in con-
4 formity with an authorization under section 102A.

5 “(2) A person moving to suppress evidence under
6 paragraph (1) shall make such motion before the relevant
7 trial, hearing, or other proceeding, unless there was no
8 opportunity to make such a motion or the person was not
9 aware of the grounds of the motion.

10 “(e) Whenever a court or other authority is notified
11 pursuant to subsection (b) or (c) of this section, or when-
12 ever a motion is made pursuant to subsection (d) of this
13 section, or whenever any motion or request is made pursu-
14 ant to any other statute or rule of the United States or
15 any State by a person who was the target of, or whose
16 communications or activities were subject to, an acquisi-
17 tion authorized pursuant to section 102A before any court
18 or other authority of the United States or any State—

19 “(1) to discover or obtain applications or orders
20 or other materials relating to an acquisition author-
21 ized pursuant to section 102A; or

22 “(2) to discover, obtain, or suppress evidence or
23 information obtained or derived from an acquisition
24 authorized pursuant to section 102A,

1 the United States district court or, where the motion
2 is made before another authority, the United States
3 district court in the same district as the authority,
4 shall, notwithstanding any other law, if the Attorney
5 General files an affidavit under oath that disclosure
6 or an adversary hearing would harm the national se-
7 curity of the United States, review in camera and ex
8 parte the application, order, and such other mate-
9 rials relating to the acquisition as may be necessary
10 to determine whether such acquisition was lawfully
11 authorized and conducted. In making this deter-
12 mination, the court may disclose to the person who
13 was the target of, or whose communications or ac-
14 tivities were subject to, an acquisition authorized
15 pursuant to section 102A, under appropriate secu-
16 rity procedures and protective orders, portions of the
17 application, order, or other materials relating to the
18 acquisition only where such disclosure is necessary
19 to make an accurate determination of the legality of
20 the acquisition.

21 “(f) If a United States district court, under sub-
22 section (e), determines that an acquisition authorized
23 under section 102A was not lawfully authorized or con-
24 ducted, it shall, in accordance with the requirements of
25 law, suppress the evidence which was unlawfully obtained

1 or derived from the acquisition or otherwise grant the mo-
2 tion of the person who was the target of, or whose commu-
3 nications or activities were subject to, an acquisition au-
4 thorized under section 102A. If the court determines that
5 such acquisition was lawfully authorized and conducted,
6 it shall deny the motion of the person who was the target
7 of, or whose communications or activities were subject to,
8 an acquisition authorized under section 102A except to the
9 extent that due process requires discovery or disclosure.

10 “(g) Orders granting motions or requests under sub-
11 section (f), decisions under this section that an acquisition
12 was not lawfully authorized or conducted, and orders of
13 the United States district court requiring review or grant-
14 ing disclosure of applications, orders, or other materials
15 relating to an acquisition shall be final orders and binding
16 upon all courts of the United States and the several
17 States, except a United States court of appeals and the
18 Supreme Court of the United States.

19 “(h)(1) Federal officers who acquire foreign intel-
20 ligence information under section 102A may consult with
21 Federal law enforcement officers or law enforcement per-
22 sonnel of a State or political subdivision of a State (includ-
23 ing the chief executive officer of that State or political sub-
24 division who has the authority to appoint or direct the
25 chief law enforcement officer of that State or political sub-

1 division) to coordinate efforts to investigate or protect
2 against—

3 “(A) actual or potential attack or other grave
4 hostile acts of a foreign power or an agent of a for-
5 eign power;

6 “(B) sabotage or international terrorism; or

7 “(C) clandestine intelligence activities by an in-
8 telligence service or network of a foreign power or by
9 an agent of a foreign power.

10 “(2) Coordination authorized under paragraph (1)
11 shall not preclude the certification required by section
12 102A.

13 “(i) Nothing in this section shall prevent the United
14 States from seeking protective orders or asserting privi-
15 leges ordinarily available to the United States to protect
16 against the disclosure of classified information.”

17 (b) TABLE OF CONTENTS.—The table of contents in
18 the first section of the Foreign Intelligence Surveillance
19 Act of 1978 (50 U.S.C. 1801 et seq.) is amended by in-
20 serting after the item relating to section 102 the following:

“102A. Authorization for acquisition of certain foreign intelligence information.

“102B. Directives relating to electronic surveillance and other acquisitions of
foreign intelligence information.

“102C. Use of information acquired under section 102A.”

21 **SEC. 4. LIABILITY DEFENSE.**

22 (a) IN GENERAL.—Notwithstanding any other provi-
23 sion of law, and in addition to the immunities, privileges,

1 and defenses provided by any other source of law, no ac-
2 tion shall lie or be maintained in any court, and no pen-
3 alty, sanction, or other form of remedy or relief shall be
4 imposed by any court or any other body, against any per-
5 son for the alleged provision to an element of the intel-
6 ligence community of any information (including records
7 or other information pertaining to a customer), facilities,
8 or any other form of assistance, during the period begin-
9 ning on September 11, 2001, and ending on the effective
10 date of this Act, in connection with any alleged classified
11 communications intelligence activity that the Attorney
12 General or a designee of the Attorney General certifies,
13 in a manner consistent with the protection of state secrets,
14 is, was, would be, or would have been intended to protect
15 the United States from a terrorist attack. This section
16 shall apply to all actions, claims, or proceedings pending
17 on or after the effective date of this Act.

18 (b) JURISDICTION.—Any action or claim described in
19 subsection (a) that is brought in a State court shall be
20 deemed to arise under the Constitution and laws of the
21 United States and shall be removable under section 1441
22 of title 28, United States Code.

23 (c) DEFINITIONS.—In this section:

24 (1) INTELLIGENCE COMMUNITY.—The term
25 “intelligence community” has the meaning given the

1 term in section 3(4) of the National Security Act of
2 1947 (50 U.S.C. 401a(4)).

3 (2) PERSON.—The term “person” has the
4 meaning given the term in section 2510(6) of title
5 18, United States Code.

6 **SEC. 5. USE OF INFORMATION.**

7 Section 106 of the Foreign Intelligence Surveillance
8 Act of 1978 (50 U.S.C. 1806) is amended—

9 (1) in subsection (i)—

10 (A) by striking “radio communication” and
11 inserting “communication”; and

12 (B) by striking “contents indicates” and
13 inserting “contents contain significant foreign
14 intelligence information or indicate”; and

15 (2) by adding at the end the following:

16 “(1) Nothing in this section shall prevent the United
17 States from seeking protective orders or asserting privi-
18 leges ordinarily available to the United States to protect
19 against the disclosure of classified information.”

20 **SEC. 6. TECHNICAL AND CONFORMING AMENDMENTS.**

21 Section 103(e) of the Foreign Intelligence Surveil-
22 lance Act of 1978 (50 U.S.C. 1803(e)) is amended—

23 (1) in paragraph (1), by striking “501(f)(1)”
24 and inserting “102B(d) or 501(f)(1)”; and

1 (2) in paragraph (2), by striking “501(f)(1)”
2 and inserting “102B(d) or 501(f)(1)”.

3 **SEC. 7. CONSTRUCTION; SEVERABILITY.**

4 Any provision of this Act, or any amendment made
5 by this Act, held to be invalid or unenforceable by its
6 terms, or as applied to any person or circumstance, shall
7 be construed so as to give it the maximum effect permitted
8 by law, unless such holding shall be one of utter invalidity
9 or unenforceability, in which event such provision shall be
10 deemed severable from this Act and shall not affect the
11 remainder thereof or the application of such provision to
12 other persons not similarly situated or to other, dissimilar
13 circumstances.

14 **SEC. 8. EFFECTIVE DATE; TRANSITION PROCEDURES; SUN-**
15 **SET.**

16 (a) **EFFECTIVE DATE.**—Except as otherwise pro-
17 vided, this Act and the amendments made by this Act shall
18 take effect on the date of the enactment of this Act.

19 (b) **TRANSITION PROCEDURES.**—

20 (1) **EXISTING ORDERS AND REAUTHORIZA-**
21 **TIONS.**—Notwithstanding any other provision of this
22 Act—

23 (A) any order issued pursuant to the For-
24 eign Intelligence Surveillance Act of 1978 (50
25 U.S.C. 1801 et seq.) in effect on the date of the

1 enactment of this Act shall remain in effect
2 until the date of expiration of such order; and

3 (B) at the request of the applicant, the
4 court established under section 103(a) of such
5 Act (50 U.S.C. 1803(a)) shall reauthorize such
6 an order if the facts and circumstances con-
7 tinue to justify issuance of such order under the
8 provisions of such Act, as in effect on the day
9 before the date of the enactment of this Act.

10 (2) NEW APPLICATIONS.—An applicant may file
11 a new application for an order issued pursuant to
12 the Foreign Intelligence Surveillance Act of 1978
13 (50 U.S.C. 1801 et seq.) and the court established
14 under section 103(a) of such Act (50 U.S.C.
15 1803(a)) shall enter an order granting the applica-
16 tion if the application meets the requirements for an
17 order under the provisions of such Act, as in effect
18 on the day before the date of the enactment of this
19 Act.

20 (3) EXTANT AUTHORIZATION.—The court es-
21 tablished under section 103(a) of the Foreign Intel-
22 ligence Surveillance Act of 1978 (50 U.S.C.
23 1803(a)) shall extinguish any extant authorization to
24 conduct electronic surveillance or physical search en-

1 tered pursuant to such Act, at the request of the ap-
2 plicant.

3 (4) APPLICABLE LAW.—Any surveillance con-
4 ducted pursuant to an order entered under this sub-
5 section shall be subject to the provisions of the For-
6 eign Intelligence Surveillance of 1978 (50 U.S.C.
7 1801 et seq.), as in effect on the day before the date
8 of the enactment of this Act.

9 (c) SUNSET.—

10 (1) IN GENERAL.—Except as provided in para-
11 graph (2), sections 2, 3, 5, and 6 of this Act, and
12 the amendments made by such sections, shall cease
13 to have force or effect on December 31, 2009.

14 (2) APPLICATION OF EXISTING AUTHORIZA-
15 TIONS FOR THE ACQUISITION OF INFORMATION.—
16 Authorizations for the acquisition of foreign intel-
17 ligence information made pursuant to sections 102A,
18 102B, or 102C of the Foreign Intelligence Surveil-
19 lance Act of 1978, as added by section 3 of this Act,
20 and directives issued pursuant to such authoriza-
21 tions, shall remain in effect until the expiration of
22 such authorizations. Such acquisitions shall be gov-
23 erned by the provisions of section 102A, 102B, or
24 102C, as appropriate, and may not be deemed to
25 constitute electronic surveillance, as that term is de-

1 fined in subsection (f) of section 101 of the Foreign
2 Intelligence Surveillance Act of 1978 (50 U.S.C.
3 1801).

Hughes, Richard

From: Engel, Steve
Sent: Thursday, August 02, 2007 6:59 PM
To: [redacted] @judiciary-rep.senate.gov } b6
Cc: Eisenberg, John
Subject: Re: FISA

I'm not. The relevant deputy is John Eisenberg, who I am cc'ing with this email.

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

From: Johnson, Matthew (Judiciary-Rep) [redacted] @judiciary-rep.senate.gov } b6
To: Engel, Steve
Sent: Thu Aug 02 18:34:04 2007
Subject: FISA

Steve,

Are you involved in the FISA negotiations?

Is there anything my boss can do to help move things forward?

Thanks.

MLJ

Matthew L. Johnson
United States Senate - Committee on the Judiciary
Counsel to U.S. Senator John Cornyn

b6

[redacted]

67

Berhanu, Tsedey

From: Donesa, Chris <@mail.house.gov>] b6
Sent: Saturday, August 04, 2007 12:14 PM
To: Eisenberg, John
Subject: RE: Legislative History

Ms. Wilson just asked me to get something to her by 4 if at all possible -

-----Original Message-----
From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Saturday, August 04, 2007 11:25 AM
To: Donesa, Chris
Subject: Fw: Legislative History

When do you think they will vote on this?

----- Original Message -----
From: Gerry, Brett (OLP)]
To: Eisenberg, John;
Sent: Sat Aug 04 11:12:30 2007
Subject: Fw: Legislative History

b2
b6

Will call you on this.

----- Original Message -----
From: Donesa, Chris <@mail.house.gov>
To: Gerry, Brett (OLP)]
Cc:
Sent: Sat Aug 04 11:05:45 2007
Subject: Legislative History

b2
b6

Gents - Ms. Wilson is interested in inserting a statement of legislative history into the record to clarify any potentially ambiguous issues. I asked NSA if they had any thoughts last week, but haven't heard back. Do either of you have any thoughts or (even better) product on the subject we might be able to use?

Berhanu, Tsedey

From: Donesa, Chris
Sent: Saturday, August 04, 2007 3:45 PM
To: Eisenberg, John
Subject: RE: Legislative History

Jbb

As far as we know it is, but we hear that Hoyer is so angry about not getting his way that he refuses to acknowledge right now that a bill is even going to be brought up. A lot of standing by to stand by

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

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Saturday, August 04, 2007 3:42 PM
To: Donesa, Chris
Subject: Re: Legislative History

No prob. Do you think this is going to happen?

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

From: Donesa, Chris <
To: Eisenberg, John
Sent: Sat Aug 04 15:39:02 2007
Subject: RE: Legislative History

Jbb

Ms. Wilson has done a draft (I believe herself) covering a number of general issues setting up the basic intent of the bill, as well as reverse targeting and the two issues Brett raised. I've reviewed it and it looks good. I told her that y'all were willing to review it, but she never got back to me on that so I'm not sure if I can share it

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

From: Eisenberg, John [mailto:John.Eisenberg@usdoj.gov]
Sent: Saturday, August 04, 2007 3:25 PM
To: Donesa, Chris
Subject: Re: Legislative History

Any intel?

Message

Berhanu, Tsedey

From: Doneso, Chris [redacted] b6
Sent: Tuesday, August 07, 2007 2:22 PM
To: [redacted]@dni.gov; Gerry, Brett (OLP); Olsen, Matthew; Eisenberg, John; Roland, Sarah E; Potenza, Vito [redacted] Miller, Jonathan E. b3
Subject: Hoekstra Open Letter to NYT b2
Attachments: FISA - NYT Letter 080707.pdf b6

Attached. Happy Tuesday to all!

SILVESTRE NEVES, TEXAS, CHAIRMAN
ALCEE L. HASTINGS, FLORIDA, VICE CHAIRMAN
LEONARD L. ROBYNELL, IOWA
ROBERT E. BISHOP, ALABAMA
ANNA G. ESCOBAR, CALIFORNIA
BUSH D. HOLT, NEW JERSEY
C.A. DUTCH BLANKENHORN, MARYLAND
JOHN E. TIERNEY, MASSACHUSETTS
MIKE THOMPSON, CALIFORNIA
JAMES B. SCHAKOFSKY, ILLINOIS
JAMES H. LANGRISH, MISSISSIPPI
PATRICK J. MURPHY, PENNSYLVANIA
PETER SCOTT, ILLINOIS, LEADING MEMBER
TERRY L. GIBSON, ARIZONA
KEITH WILSON, MISSISSIPPI
MATT THOMPSON, TEXAS
JOHN J. WHELAN, NEW YORK
TOMMY DANIEL, TENNESSEE
ANTHONY CAROLLO, MISSOURI
RICK WENZ, ARIZONA
GABRIEL L. GONZALEZ, CALIFORNIA

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

H-405, The Capitol
Washington, DC 20515
(202) 225-7600

MICHAEL OTTENS
STAFF DIRECTOR
TIMOTHY W. HENNING
MANAGING SECRETARY

August 7, 2007

NANCY PELOSI, SPEAKER
JOHN A. BOEHNER, REPUBLICAN LEADER

Mr. Bill Keller
Executive Editor
The New York Times
620 Eighth Avenue
New York, NY 10018

Dear Mr. Keller:

It has been my practice not to deal with the New York Times after its recklessness in repeatedly disclosing highly classified intelligence programs to enemies who seek to attack our nation and because of what I believe was a lack of honesty and integrity in its dealings with me as Chairman of the Committee at that time.

However, I believe that your Editorial this morning "The Fear of Fear Itself" and an article that ran yesterday purporting to describe legislation to clarify the Foreign Intelligence Surveillance Act ("FISA") supported in the House of Representatives to address an urgent intelligence gap so misled the American people as to require urgent correction. The only real basis for "fear" here is the scare tactics being perpetuated by the Times, which has knowingly and willfully misrepresented the new law to scare the American people.

Before moving to a point-by-point rebuttal based on the actual text of the new law, extensive experience with FISA, and knowledge of the actual facts at issue not available to the Times, I would like to also address two broader points. First, the legislation was intended to address significant and substantial intelligence gaps that have arisen at a time of enhanced threat of terrorist attack on the United States. The need for the bill was urgent and obvious. DNI McConnell repeatedly emphasized that "we are missing a significant portion of what we should be getting" to detect and prevent terrorist attacks. Bipartisan recognition of the need for this bill is why it passed both the House and the Senate so quickly.

And the recently released key judgments of a National Intelligence Estimate clearly emphasized that the United States is in a time of enhanced threat from Al Qaeda, which still is planning "high-impact plots" "likely to continue to focus on prominent political, economic and infrastructure targets with the goal of producing mass casualties." Had we not passed this law and an attack not been prevented, I'm sure that the New York Times would have been first in line to criticize the failure to "collect the dots", much less to "connect the dots".

Second, it is unfortunate that you so completely disregard the professional judgments of DNI McConnell, other Intelligence Community professionals, and even indications from

judges of the FISA Court itself that this legislation was urgently needed to close intelligence gaps and better focus the FISA process on protecting the civil liberties of Americans instead of radical jihadist overseas. Director McConnell — who served as NSA Director under President Clinton — deserves praise for repeatedly emphasizing that FISA reforms must balance intelligence needs with the civil liberties of Americans. His personal involvement and guidance of this process at every step were critical in making it happen and he deserves praise for his effectiveness and professionalism instead of ugly personal attacks. There is no evidence whatsoever that any alleged "agreement" was reached with congressional Democrats, and there is no cause to name Admiral McConnell based on hearsay.

Below, I have corrected a number of spelling mistakes and exaggerations in your August draft and in this morning's editorial. Any of them should have been readily apparent from a cursory look at the text of the law itself, but unfortunately your newspaper chose fear mongering over what might be happening rather than the facts and what the law actually says.

Article

Mistatement and Exaggeration — impact went far beyond the small fixes that administration officials had said were needed to gather information about foreign terrorists.

- a. Points FISA is an extremely complex statute that is difficult enough to understand and apply even when it is not being deliberately distorted. Unfortunately, instead of requiring the law, the New York Times chose to make up new assertions wholly unsupported by the facts. This did a disservice to our intelligence professionals who are attempting to keep America — especially prominent targets such as New York — safe.
- b. The new law plainly and expressly provides that surveillance must be directed at (or targeted to) a person reasonably believed to be located outside the United States. Under well-established FISA practice and precedent, this only permits surveillance of foreign targets on foreign soil, not Americans on American soil. The intelligence community must develop procedures to answer this in the case, and those procedures must be reviewed by the FISA Court.
- c. Any surveillance targeting Americans in the United States would still require an individual warrant from the FISA court, and any incidental collection of the communications of U.S. persons would still be subject to extensive minimization procedures. The bill expressly requires such minimization procedures to be imposed on any surveillance conducted under the new law, and those procedures must also be reviewed by the FISA court.
- d. Congresswoman Watson expressly clarified in the Congressional Record that so-called "reverse targeting" of the communications of Americans is intended to be illegal under this bill. Director McConnell also repeatedly has stated his

intent in congressional briefings to seek an individualized order of the FISA Court to target any communication of an American.

- o Judges of the FISA Court itself have also clearly expressed frustration with the fact that so much of their workload is consumed by applications that focus on foreign targets and involve minimal privacy interest of Americans.

- Misstatement and Exaggeration. The new law for the first time provided a legal framework for much of the surveillance without warrants that was being conducted in secret by the National Security Agency and outside the Foreign Intelligence Surveillance Act, that is supposed to regulate the way the government can listen to the private communications of American citizens.

- o Facts. The Attorney General has publicly disclosed that the activities previously conducted under the Terrorist Surveillance Program described by the President were now all completely under FISA. The new law applies only to surveillance targeted at foreign persons, and a FISA order would continue to be necessary for surveillance targeted at Americans. The current FISA structure can handle these applications with speed and agility.

- Misstatement and Exaggeration. FISC still classified ruling earlier this year which said the government needed to seek court-approved warrants to monitor those international calls going through American switches.

- o Facts. It's not necessary to address or discuss any alleged court opinion to demonstrate that this assertion is false. The FISA modernization legislation passed by the House in the 109th Congress -- well before the alleged opinion -- attempted to address and close the FISA loophole for foreign terrorists.

- Misstatement and Exaggeration. If the court's only role will be to review and approve the procedures used by the government in the surveillance after it has been conducted.

- o Facts. This is a false and selective characterization of the plain provisions of the law. Third parties who are asked to assist the intelligence community under the law may challenge the legality of any objective by filing a petition with the FISA Court.

Editorial

- Misstatement and Exaggeration. [T]oo scared of Republican campaign ads to use it to protect the Constitution.

- o Facts. Even without addressing the obvious fact that radical jihadists in foreign countries are not entitled to privacy rights under the Constitution relating to foreign intelligence collection, courts that have addressed the issue to date have made clear they believe that the type of surveillance

contemplated by the bill is fully consistent with the Constitution, including the Fourth Amendment.

- Minimalist and Exceptional - They gave the Director of National Intelligence and his attorney general authority to intercept - without warrants, court supervision or accountability - any telephone call or e-mail message that moves in, out of or through the United States as long as there is a reasonable belief that one party is located in the United States.

c. Proof - This assertion is false under the express terms of the statute. The law clearly requires that the surveillance be directed at (a) an individual (b) to persons located in the United States, and that procedures be in place to allow review by the FISA Court to ensure that surveillance programs do not cover persons outside the United States. In addition, the law requires minimization procedures reviewed by the FISA Court to be in place to deal with incidental collection of communications of Americans.

- Misstatement and Exaggeration - It would allow the government to intercept without warrant every communication in, to or out of any country including the United States.

d. Limit - In this case, the FISA Court would be virtually shut down. We will expect the Court to be conducting a significant and independent volume of work to protect the privacy interests of Americans. If this bill is passed, it should:

Protecting America at a time of increased threat continues to pose great challenges for our Intelligence Community and our citizens. It is important that you choose to compound these difficulties with further politicization, harassment, and the suggestion that we simply dismiss the increased threats to American citizens at home and abroad.

Sincerely,



Peter Hoekstra
Ranking Republican

follow up

Hughes, Richard

From: Bash, Jeremy] b6
 Sent: Wednesday, August 08, 2007 12:55 PM
 To: Ben Powell; Eisenberg, John (OLP); Potenza, Vito] Olsen, Matthew; Gerry, Brett b6
 Cc: Parker, Wyndee; Donesa, Chris; Delaney, Mike; Lowry, Ashley
 Subject: Follow up

Gang,

First, I want to thank you all very much for the assistance you provided our Members during the activity on FISA over the last few weeks. I can't think of a single time that you were unresponsive to a question or an ask. We couldn't have produced any legislation without you. So, thank you.

Second, tomorrow morning a bipartisan staff delegation from HPSCI is going to go to NSA to discuss the new authority and its implementation. I need to clarify today some of the clearance issues. What clearance will be required for the discussion? TSP? SI/TK only?

Part of the reason I raise this is that we understand that SSCI has been granted 12 slots for TSP. We have 8 (not counting security/steno). Given that our Committee is larger than SSCI, it only makes sense for us to expand our TSP access as well. I am awaiting some feedback from Chris D on how many individuals the Ranking Member would like read in, but from our side, we thought a good arrangement would be to add 5 (3 majority, 2 minority). This would bring our total to 13.

If I can get the green light from you on this today, we can do some of the read-ons tomorrow. If I can't get the green light today, can you at least assure me that HPSCI staff with SI/TK (and a need-to-know as determined by staff directors) can have access to the (1) court orders; and (2) activities under the New FISA authority?

Under separate cover, you'll also be hearing (or have heard) from Mike, Wyndee et al about our hearing schedule in September.

Thanks.

- Jeremy

Jeremy Bash | Chief Counsel

House Permanent Select Committee on Intelligence

[] b6
 []
 []

Hughes, Richard

From: Parker, Wyndee [] b6
 Sent: Monday, August 20, 2007 11:43 AM
 To: Eisenberg, John
 Cc: Apelbaum, Perry [] @dni.gov; Bash, Jeremy; Delaney, Mike; Roland, Sarah E; Olsen, Matthew; Bradbury, Steve; DeBacá, Lou b2
 Subject: Email follow up per your request
 Follow Up Flag: Follow up
 Flag Status: Red

All: When we spoke to Ken last week he referred us to OLC for the latest update re: our outstanding TSP/FISA document requests.

John: Thank you for setting up the meeting with the key entities regarding these requests. Again, ideally we hope to meet with you this week.

Perry Apelbaum's number is [] b6

Many thanks,

Wyndee Parker

Deputy Staff Director and General Counsel

House Permanent Select Committee on Intelligence

The Capitol, Room H-405

Washington, DC 20515

) b6