Turner, Kathleen

From: Turner, Kathleen
Sent: Wednesday, January 30, 2008 6:34 PM
To: Healey, Louise C; Livingston, John R; Wolfe, James
Cc: [redacted]
Subject: [redacted] Info Requested by Chris Healey

(b)(1)
(b)(3)

[redacted]

Chris: Per your request, the following is provided:

[redacted]

John –
Section 407 of the Administration's FISA modernization proposal would have amended the statutory definition of "agent of a foreign power" to include individuals involved in the international proliferation of weapons of mass destruction.
Ken Wainstein highlighted this provision in his testimony last September.
As you may know, since the proposal was first circulated, questions have been raised about why broadening this definition was necessary and whether there have been any actual cases where the government was not able to obtain a FISA order for an individual involved in the international proliferation of catastrophic WMD.
If you or your colleagues could provide me with this information about this, or direct me to something you have already submitted to the Committee, it would be very helpful.
Thanks,
Chris

Classified By:

Classification Reason:

Declassify On:

9/11/2008

Questions for the Record for the
Hearing on Implementation of the Protect America Act
and
Foreign Intelligence Act Amendments
September 20, 2007

Implementation Issues

Question 1. (TS//SI//NF) The DNI and AG have issued

- **How many additional certifications are planned under the Protect America Act?**
- **Will each certification be governed by the identical procedures for determining the reasonableness of "foreign-ness"?**
- **Do the [redacted] or any additional certifications that are planned, present different questions in terms of implementation of the Act? Please explain.**

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Answer: (TS//SI//NF)

(TS//SI//NF) With respect to the procedures used for determining that the acquisition of foreign intelligence information concerns persons reasonably believed to be located

[redacted]

outside the United States [redacted]

[redacted] However, the Government could, in the course of its implementation and oversight activities, identify aspects of the procedures that it might deem appropriate to modify in the future.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Question 2: (S//SI//NF) Mr. Wainstein's statement for the record states that the Department is awaiting the FISA Court's review of the foreign-cess procedures.

- Has DOJ submitted to the Court a formal application to request the Court's review and approval? If so, has this or could this application be shared with the Committee?
- What have been the interactions with the FISA Court to date with respect to that review?
- Has DOJ been given any indication when the Court review will be completed?
- Has the FISA Court issued any orders or opinions since passage of the Protect America Act that bears on the legislation?

Answer: (U) Answers will be forth coming.

Question 3: (TS//SI//NF) Is the NSA the only agency that is now conducting acquisition activities under the Protect America Act?

[redacted]

[redacted]

- Is consideration being given to authorize the FBI to acquire foreign intelligence information under the Act?
- How broadly does the scope of the Protect America Act reach in terms of the agencies of government that can be authorized to acquire foreign intelligence information under its terms?

Answer: (TS//SI//NF)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(TS//SI//NF) Since passage of the Protect America Act, the Intelligence Community has been implementing the authorities authorized by the Act in coordination with an interagency working group comprised of representatives from the Office of the Director of National Intelligence. [redacted]

(TS//SI//NF)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(TS//SI//NF) With respect to FBI, at this time, the FBI does not assess that it has a critical mission need to obtain authority under the Protect America Act in order to fulfill its national security mission inside the United States; although it is currently evaluating whether it does require authority to access to certain unminimized information in support of its counterterrorism mission. Of course, the information obtained under the Protect America Act by other agencies may be critical to FBI operations. Existing laws and regulations mandate sharing of critical information, such as counterterrorism information, with the FBI to carry out the FBI's national security mission. The FBI continues to make extensive use of FISA electronic surveillance and physical search authorities under the

jurisdiction of the Foreign Intelligence Surveillance Court. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted] The Protect America Act does not specify which agencies may conduct acquisitions as approved by the Attorney General and Director of National Intelligence. Accordingly, authorization will be granted to agencies consistent with their existing authorities, roles and responsibilities under applicable statutes and Executive Orders.

Question 4: [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

- Please explain any difference.
- How does each set meet the requirements for minimization procedures under FISA section 101(h)?

Answer: (U) Answers will be forth coming.

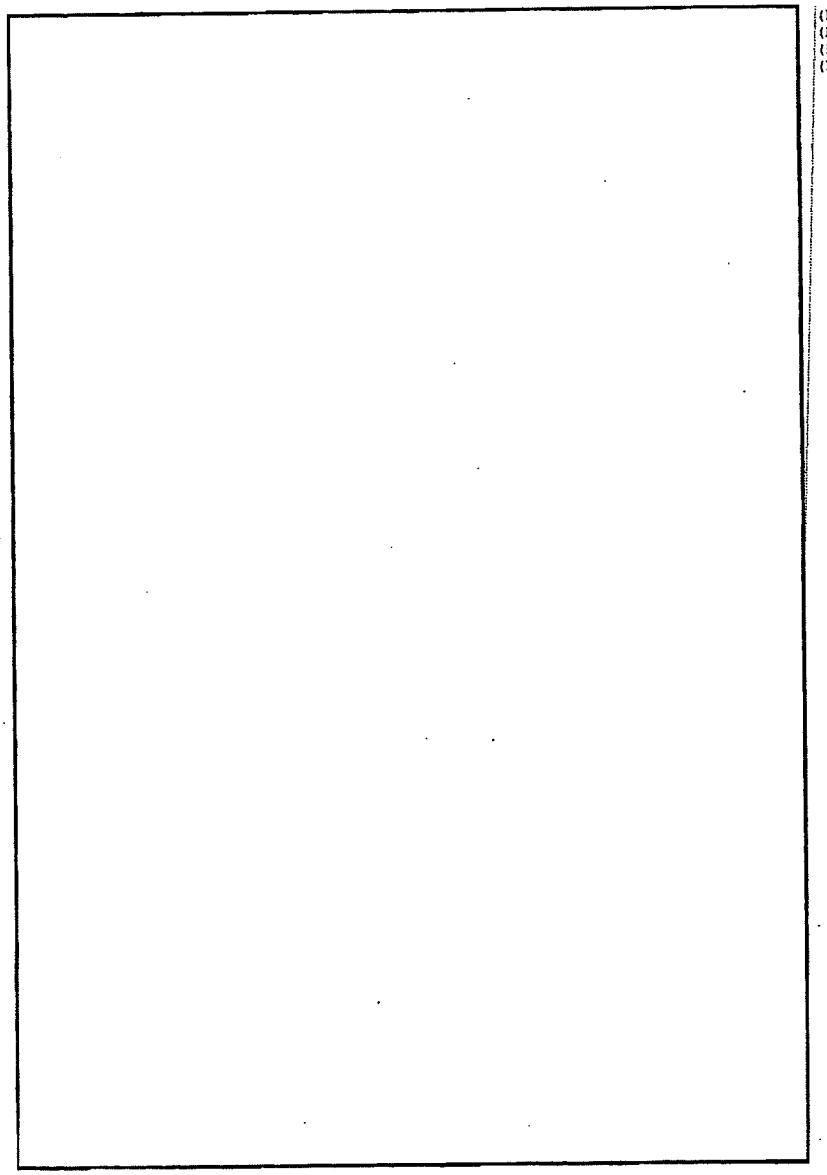
Question 5: [redacted]

[redacted] Do these procedures require the destruction of the information acquired in these circumstances?

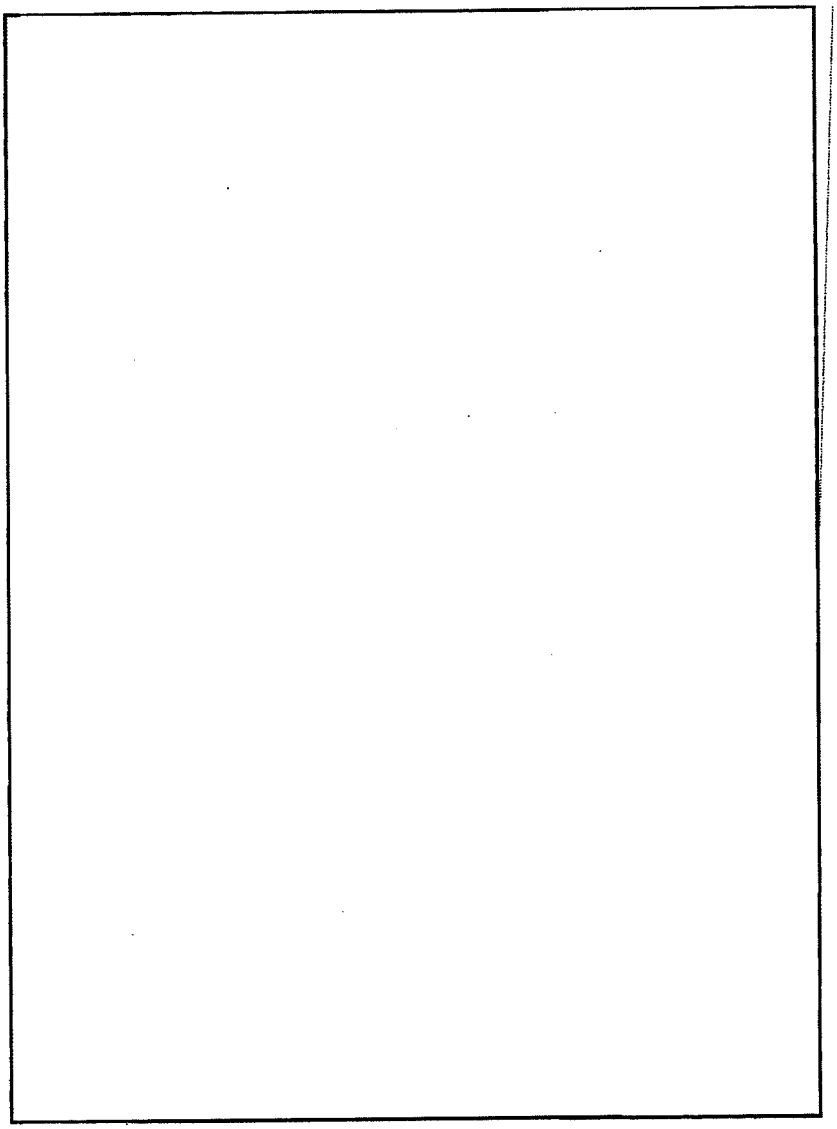
Answer: [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Question 7: (U) The witnesses testified that the Government will operate under section 2.5 of Executive Order 12333. DNI McConnell said: "To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad." Is it the position of the Department of Justice that the new law could be interpreted to release the U.S. Government from the requirement set forth in section 2.5 that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power before the Intelligence Community may conduct electronic surveillance or physical search of that person?

Answer: (U) Answers will be forth coming.

Question 8: (TS//SI//NF) The NSA procedures for collection under the Protect America Act provide for the NSA Director to "take action in apparent departure from these procedures" in circumstances where the action is being to [sic] taken "in order to protect against an immediate threat to the national security" and "it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence[.]"

- What departures from these procedures would be permissible under the Protect America Act?
- What mechanisms exist to ensure that this provision is not abused?
- Would the Administration support a proposal requiring that the Foreign Intelligence Surveillance Court receive notice of when this provision is used and have oversight of its use?

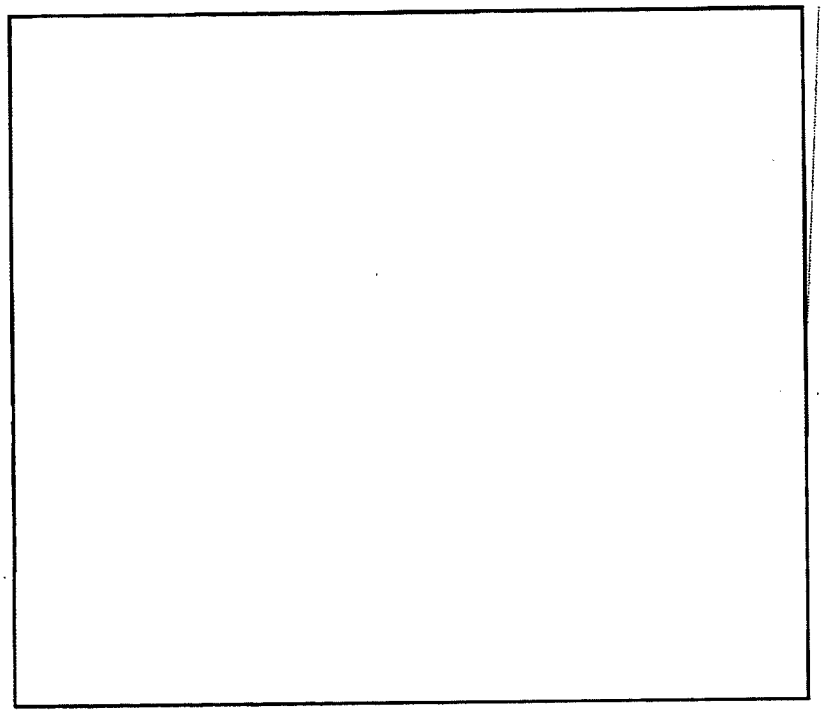
Answer: (TS//SI//NF) A departure from the foreign targeting procedures could encompass circumstances where any of the requirements of the procedures, except those that are required by the Act itself – such as the requirement that the acquisition concern persons reasonably believed to be located outside the United States – could be departed from "in order to protect against an immediate threat to the national security." For example, the procedures have requirements concerning the timing of oversight reviews (14 and 60 days). If, for example, a heightened threat environment required the diversion of oversight personnel to operational matters, a scheduled review could be delayed under this provision to meet operational needs. In addition, a significant departure may also constitute a "significant intelligence activity" and an appropriate notification to Congress would be provided pursuant to the National Security Act of 1947, as amended.

(TS//SI//NF) The procedures themselves contain an important mechanism to ensure that this provision is not abused. Specifically, the procedures state that if this provision is invoked, "…NSA shall report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer." Accordingly, due to this threefold reporting requirement, the Intelligence Community is confident that this provision will not be abused. Due to

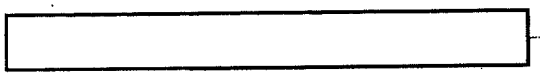
this extensive internal Executive Branch oversight, we believe that additional Court notice and review is unnecessary. As of January 18, 2008, this provision has not been used.

Question 2: [redacted] Is there any kind of acquisition which prior to the Protect America Act had been considered to be a search under the FISA which may now be conducted without a FISA search order?

Answer: (U) Answers will be forth coming.



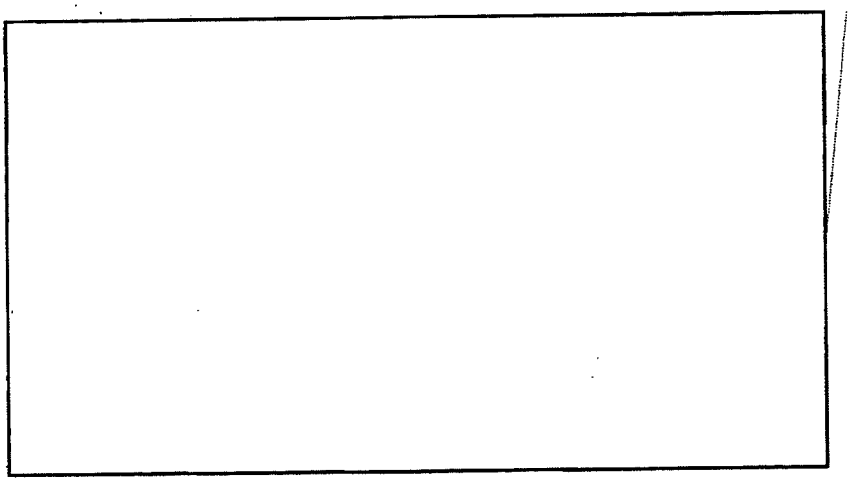
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

- **(U) How does the Department of Justice define "stored communications" and what legal questions is the Department now considering concerning the acquisition of that data under the Protect America Act?**

Answer: (U) Answers will be forth coming.



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

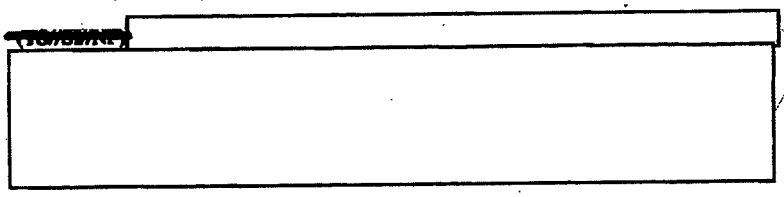
- **(TS//SI//NF) What is the proper role of the NSA in light of the fact that it is not permitted to conduct searches in the United States?**

Answer: (U) Section 105B(a)(3) of the Protect America Act provides that:

> The acquisition involved obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications[.]

Accordingly, the Act provides for the acquisition of stored communications.

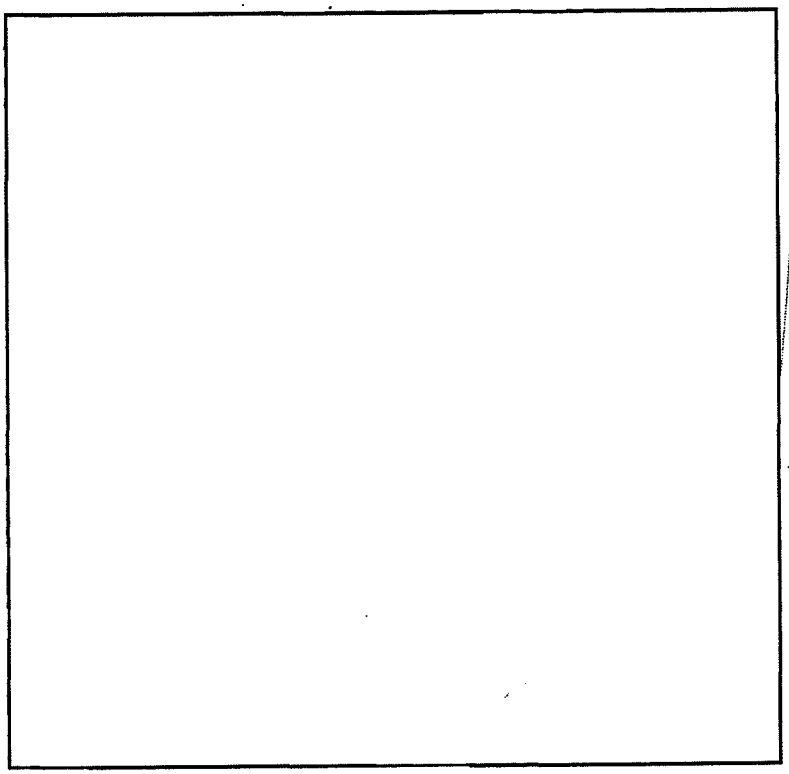
(TS//SI//NF)



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

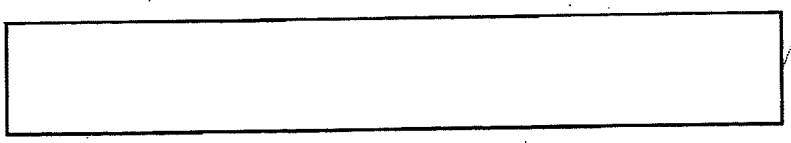
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Question 11: ~~(TS//SI//NF)~~ **Please provide statistics on the number of communications collected under the Protect America Act that have incidentally captured a U.S. Person communication. Understanding that NSA may not be able to give a precise answer, does the Agency have an estimate on this? If not, is there any way to extrapolate an estimate by looking at other NSA collection programs that target persons outside the United States?**



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[2] E.g., Domestic communications, communications between two U.S. persons, communications of the U.S. Government.

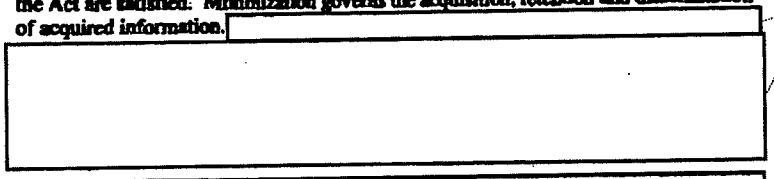


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(S//NF) More Meaningful Measures of U.S. Person Information Collected: A more quantitative and meaningful metric could be derived from the application of our minimization procedures, which are in place to govern the process NSA follows when it collects, processes, retains, and disseminates foreign intelligence to, from, or about a U.S. person. Our minimization procedures, approved by the Attorney General and shared with the intelligence committees, permit the dissemination of information that identifies a U.S. person if that information meets two tests: it is evaluated to be foreign intelligence, and the identifying information is necessary to understand or assess the foreign intelligence information. In the overwhelming majority of cases, however, NSA masks the U.S. identity when we disseminate foreign intelligence in an intelligence report. Consequently, we capture the number of intelligence reports we issue that contain minimized and masked U.S. person information, as well as the number of times SIGINT customers request the minimized U.S. identity. These measures have proven over the years to be an effective way to protect U.S. privacy and are very conducive to regular reporting to our overseers.

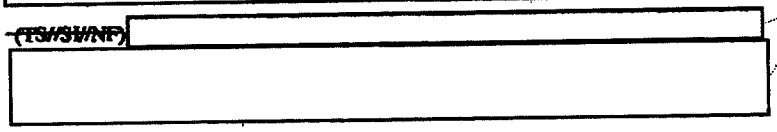
Question 12: (TS//SI//NF) For communications where the non-targeted party is a U.S. Person, and that U.S. Person never himself becomes a target, does the law allow that collection, with minimization, to continue forever? Would you accept a statutory requirement that NSA have an internal review of those communications to make sure that they continue to provide foreign intelligence, that the minimization procedures are applied, and that the U.S. Person is not a target (as such a review already appears to be required by USSID 18, section 5.2)?

Answer: (TS//SI//NF) The Protect America Act requires that a significant purpose of the acquisition conducted under the Act be to obtain foreign intelligence information. Section 105B(a)(4). Accordingly, the Protect America Act allows for acquisition to occur as long as the target is of foreign intelligence value and the other requirements of the Act are satisfied. Minimization governs the acquisition, retention and dissemination of acquired information.

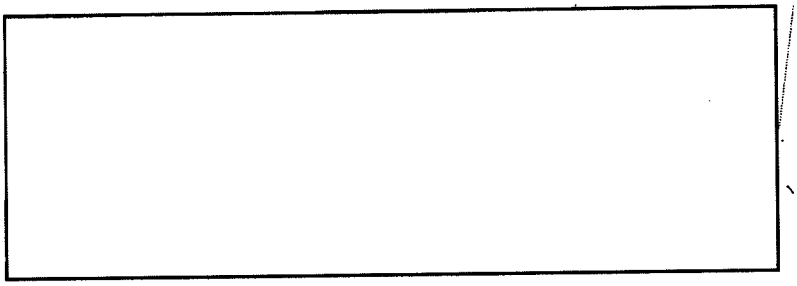


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

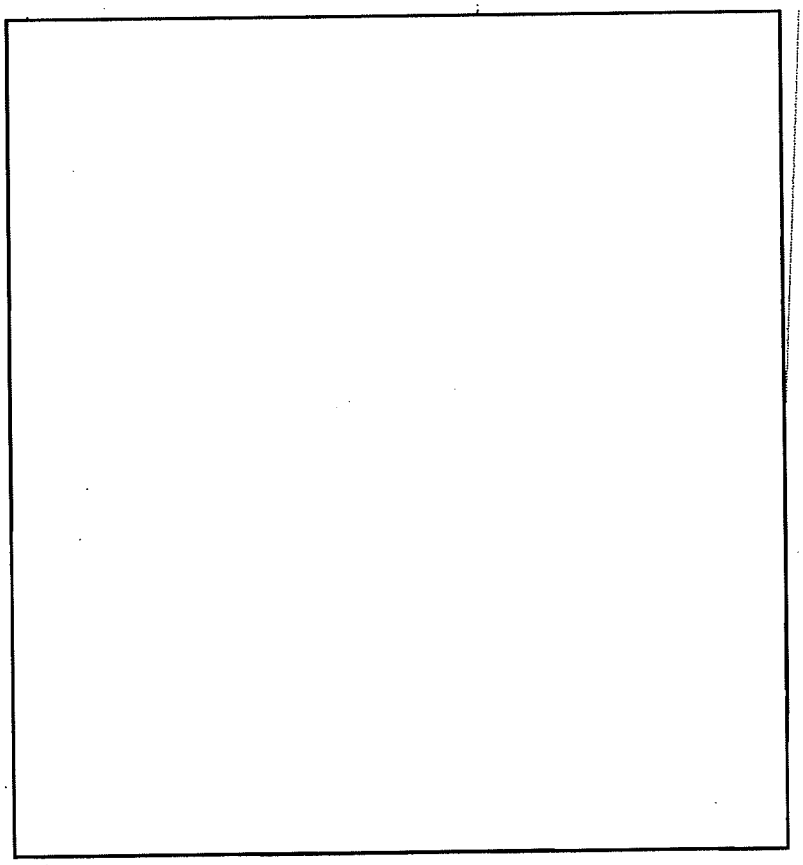
(TS//SI//NF)



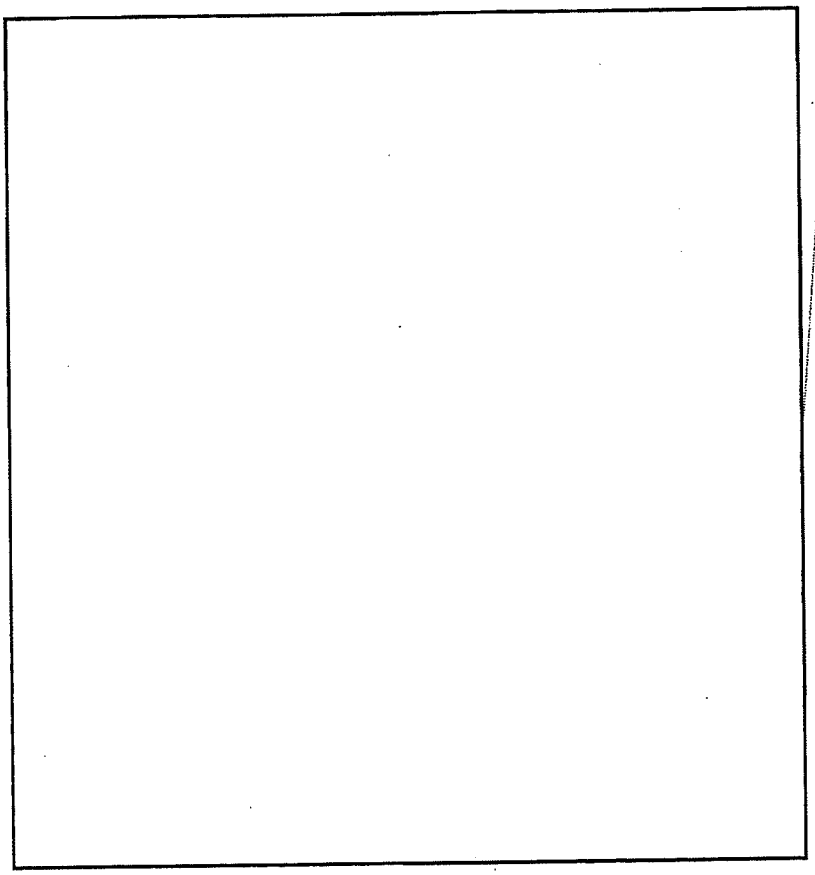
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Question 14: (U) Please provide copies of guidelines, directives and training materials related to reverse targeting and the determination about "who is the real subject of the surveillance." Please provide copies of any memorandum of law or legal opinions, including OLC documents, and any FISA Court orders, opinions or decisions on this topic with associated pleadings and memoranda of law.

Answer: (U) We respectfully refer the Committee to the specific agencies for copies of individual guidelines, directives and training materials related to reverse targeting and the determination about "who is the real subject of the surveillance." With respect to copies of any memorandum of law or legal opinions, including OLC documents, and any FISA

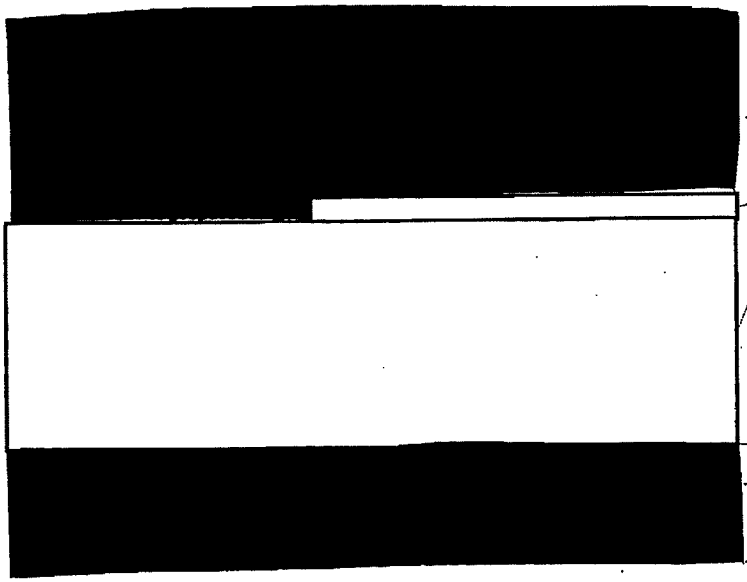
Court orders, opinions or decisions on this topic with associated pleadings and memoranda of law, we refer the Committee to the Department of Justice.

Question 15: ~~(TS//SI//NF)~~ Are there any limitations imposed by the PAA on the kind of information collected, as long as the target is overseas? Can the NSA collect business, medical records, library or bookseller, or tax records as long as they are sent by the wire to an appropriately selected target?

Answer: (U) Answers will be forth coming.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



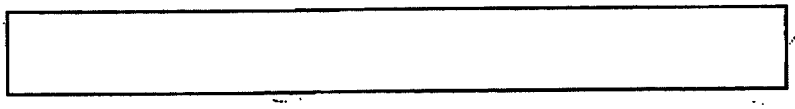
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Question 18: [redacted] The NSA may "in order to protect against an immediate threat to the national security...take action in apparent departure" from established procedures. Under what circumstances can this, or has this provision been invoked?

Answer: [redacted] As of January 18, 2008, this provision has not been invoked. It is intended to offer an avenue for handling emergency situations that are not foreseeable. If this provision were invoked in the future, the foreign targeting procedures require that NSA promptly report that activity to the Department of Justice and Office of the Director of National Intelligence.

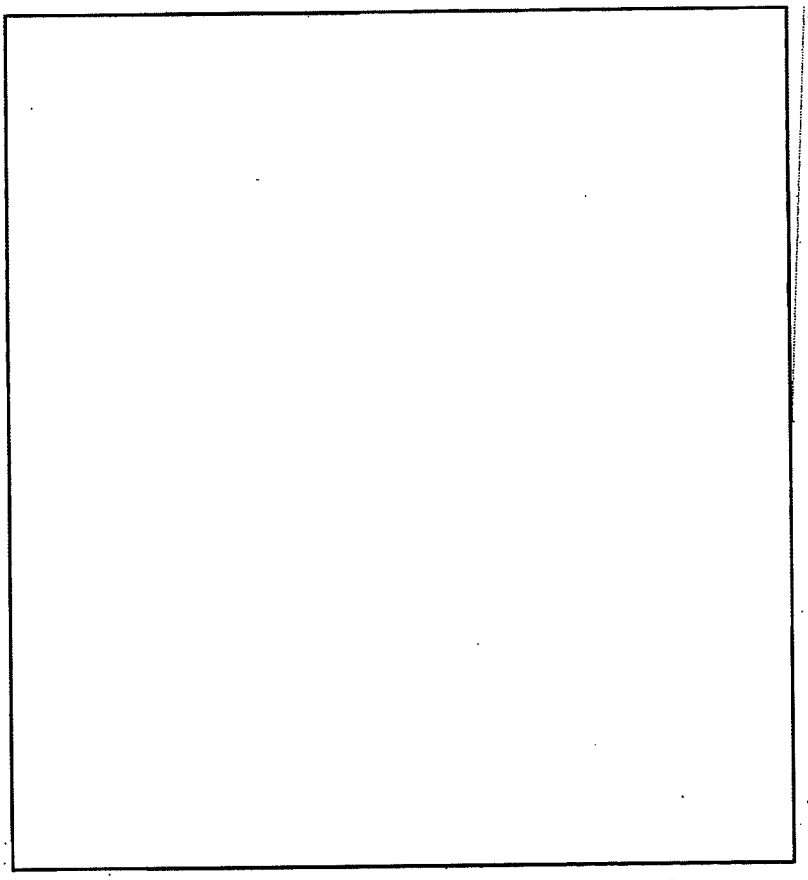
Question 19: [redacted] The DNI told Congresswoman Schakowsky that the Intelligence Community would provide information about how much U.S. person information is looked at by an analyst or other person. Please provide the Committee with this information

Answer: [redacted] In response to Rep Schakowsky's question, "How frequently does U.S. person information get collected under the Act?" the following response was provided:



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



~~(S//NF)~~ **More Meaningful Measures of U.S. Person Information Collected:** A more quantitative and meaningful metric could be derived from the application of our minimization procedures, which are in place to govern the process NSA follows when it collects, processes, retains, and disseminates foreign intelligence to, from, or about a U.S. person. Our minimization procedures, approved by the Attorney General and shared with the intelligence committees, permit the dissemination of information that identifies a U.S. person if that information meets two tests: it is evaluated to be foreign intelligence, and the identifying information is necessary to understand or assess the foreign intelligence information. In the overwhelming majority of cases, however, NSA masks the U.S. identity when we disseminate foreign intelligence in an intelligence report. Consequently, we capture the number of intelligence reports we issue that contain

[redacted]

minimized and masked U.S. person information, as well as the number of times SIGINT customers request the minimized U.S. identity. These measures have proven over the years to be an effective way to protect U.S. privacy and are very conducive to regular reporting to our overseers.

Question 20: (U) Under the Protect America Act the Attorney General and the Director of National Intelligence can authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." Please explain the intent behind the use of the word "concerning" and what would be the effect of substituting phrases such as "directed at" and "targeting" in its place.

Answer: (U) Answers will be forth coming.

Liability Issues

Question 1: (U) Does the Administration's April proposal to provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities apply to lawsuits against the United States government or government officials? Please explain.

Answer: (U) Answers will be forth coming.

Question 1: (TS//SI//NF) Were the contents of the communications of any plaintiff in any lawsuit concerning the Terrorist Surveillance Program targeted for interception under the Terrorist Surveillance Program?

Answer: (U) Answers will be forth coming.

Streamlining the FISA Process

Question 1: (U) The Administrative Office of the U.S. Courts has submitted to the Congress the recommendation of the FISA Court that it be authorized to meet en banc. One purpose of this change would be to make the Court's decision-making more efficient and predictable as differences among the judges could be resolved more quickly.

- **(U) Does the Justice Department have a position on this proposal of the FISA Court?**

Answer: (U) Answers will be forth coming.

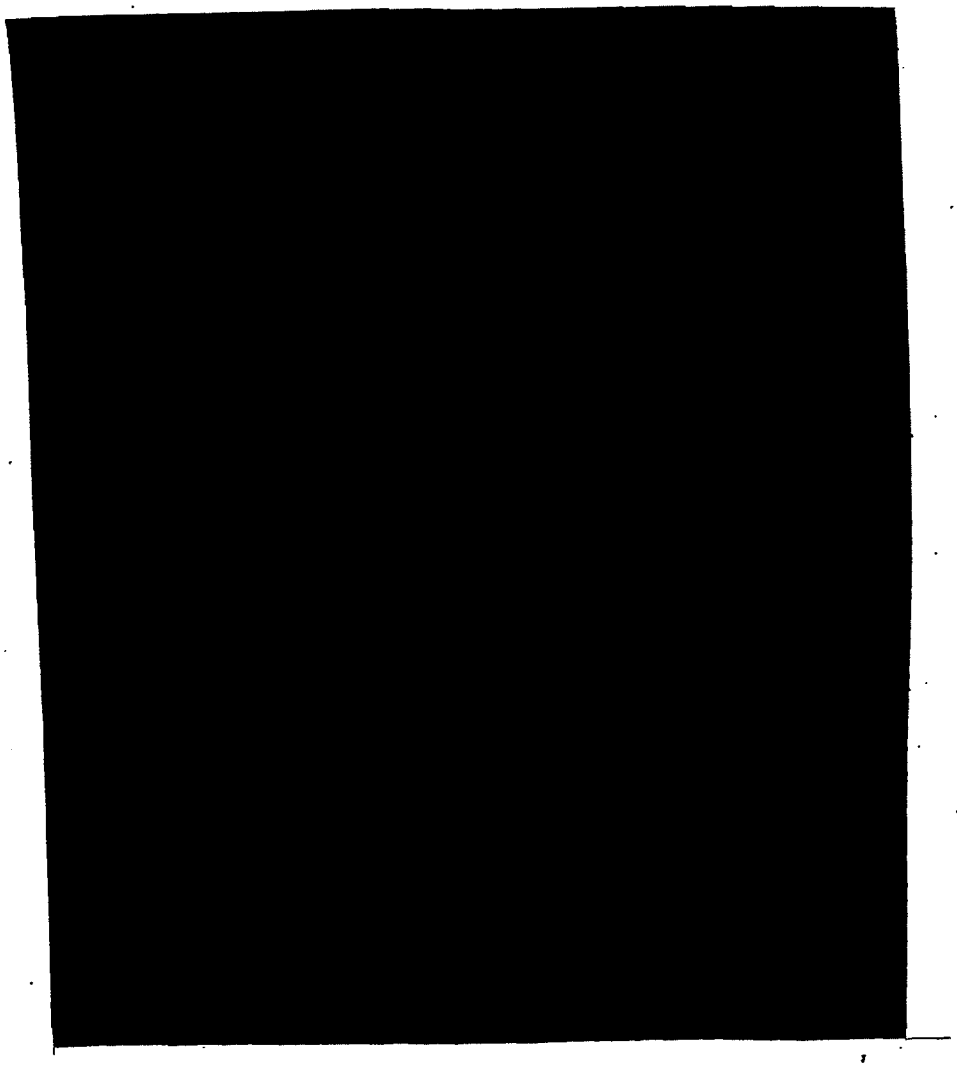
WMD Amendment to Definition of Agent of a Foreign Power

Question 1: ~~(S//NF)~~ Mr. Wainstein in his statement for the record highlighted the Administration's request that "the FISA statutory definition of 'agent of a foreign power,' the category of individuals that the Government may target with a FISA court order, be amended to included groups and individuals involved in the international proliferation of weapons of mass destruction."

- (U) Are there any examples of an actual individual involved in the international proliferation of weapons of mass destruction whom the Government cannot bring under surveillance either through a FISA order or the criminal wiretap statutes?

Answer:

[redacted]



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

FISA ISSUES
March 2006

I. FISA Issues

[redacted]

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123

[redacted]

Other FISA issues

There are two major concerns with the language of the FISA, the first of which has already been discussed above to some degree. First, because of technological advances, the current jurisdiction of the FISC goes beyond the original intent of the statute. Second, the emergency provisions of FISA do not allow for a sufficiently rapid response to emergencies. Several other problems are also worthy of discussion.

1. Jurisdiction of the FISC

Many of the issues surrounding the FISA process concern the manner in which technological advances have in effect expanded the jurisdiction of the FISC. Realigning the jurisdiction of the Court to something that better approximates what FISA covered in practical terms in 1978 -- providing protection for the privacy of communicants inside the United States -- would go a long way toward ameliorating many of the problems discussed herein.

[redacted]

[redacted]

2. Emergencies

The Attorney General must approve emergency surveillances under FISA and the FISC must ratify his authorization within 72 hours. The problem is that the people who have the facts that provide the probable cause to justify the targeting are analysts at NSA (and CIA and FBI), and going to the Attorney General necessarily takes time. Realigning the jurisdiction of the FISC would free up more resources to work on emergencies, and, most importantly, there would be far fewer emergencies if the Attorney General did not have to approve targeting directed at non-US persons outside the US. Aside from that, the time required for emergency targeting could probably be cut down only by making the DOJ approval process less onerous (by allowing people below the Attorney General to make the authorization) or (even faster) by vesting the authority for authorization in the agencies who have the facts about the threat and requiring Attorney General/FISC ratification of the authorization after the fact.

3. Other issues

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The FISA requires that the FISC be provided with a significant amount of information in requests that are submitted to it, and because the law also allows the Court to require "any additional information," many FISA applications now resemble finished

intelligence products, rather than statements of probable cause with simple descriptions of how data will be collected and handled. The Court has also imposed requirements for submission of written descriptions of new collection techniques well in advance of applications employing them, as well as other additional reporting requirements, some of which go well beyond the purview of the judiciary (justification of the foreign intelligence value of what has been collected.) Meeting these requirements takes analysts and collectors from their primary jobs, and the need for them is questionable.

* * * * * * *

II. Five example scenarios

The definitions of "electronic surveillance" in FISA require that one look at a number of factors to analyze the 5 scenarios described: the identity of the target, the location of the target, the type of communications being collected, and the location of collection. Thus, each of the scenarios has a variety of outcomes depending on how these factors are combined

1. **Collection of a communication between a point inside the United States and a point outside the United States if the collection occurs outside the United States**

   Under these circumstances:

- If the target of the surveillance were a US person inside the United States, the surveillance would fall within the first FISA definition of electronic surveillance (1801(f)(1)), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States. Therefore, a Court Order would be required.

- If the target of the surveillance were a non-US person outside the United States, none of the definitions of electronic surveillance in FISA would apply. Therefore, no Court Order would be required.

- If the target of the surveillance were a US person outside the United States, none of the definitions of electronic surveillance in FISA would apply. Therefore, no Court Order would be required. However, Attorney General approval would be required by E.O. 12333 to target such communications.

- If the target of the surveillance were a non-US person inside the United States, FISA would not apply, but Attorney General approval would ordinarily be required for the targeting if the means of communication was one in which this person would have a reasonable expectation of privacy. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

2. **Collection of a communication between a point inside the United States and a point outside the United States if the collection occurs inside the United States**

Under these circumstances:

- If the target of the surveillance were a US person inside the United States, the surveillance would fall within the first definition of electronic surveillance (1801(f)(1)), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States.
- If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance irrespective of the "US person" status of either communicant.
- If the target of the surveillance were a non-US person, or were a person outside the US, and the communications were collected while being transmitted by radio signal, FISA would not apply.
- If the communication were collected inside the United States by means other than intercept of a radio signal or collection from a wire or like connection, as above, FISA would still apply if the collection were effected through installation or use of some other surveillance device under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (e.g. installation and use of an implant on a computer within the United States).
- If the target of the surveillance were a US person outside the United States, FISA would not apply, but Attorney General approval would be required to do the targeting.
- If the target were a non-US person inside the United States, and NSA were seeking to intercept his international radio communications, FISA would not apply and no Court Order would be required. However, Attorney General approval would ordinarily be required for the targeting. [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

3. **Collection of a communication between a non-US person inside the United States and a point outside the United States, collection occurring anywhere**

Under these circumstances:

- If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance (1802(f)(2)), irrespective of the "US-person" status of the communicants.

- If the communication were being collected within the United States by means other than intercept of a radio signal or collection from a wire or like connection, FISA would still apply if the collection occurred through installation or use of some other surveillance device under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (e.g. installation and use of an implant on a computer within the United States) (see 1804(f)(4).

- If the communication were being collected outside the United States, or while being transmitted by radio signal (either within the United States or outside the United States), FISA would not apply, and no Court Order would be required.

- If the target were a US person outside the United States, FISA would not apply and no Court Order would be required. However, Attorney General approval would be required by E.O. 12333 to target such person's communications.

- If the target were a non-US person inside the United States, and NSA was seeking to intercept his international radio communications, FISA would not apply and no Court Order would be required. However, Attorney General approval would ordinarily be required to target such an individual's communications.

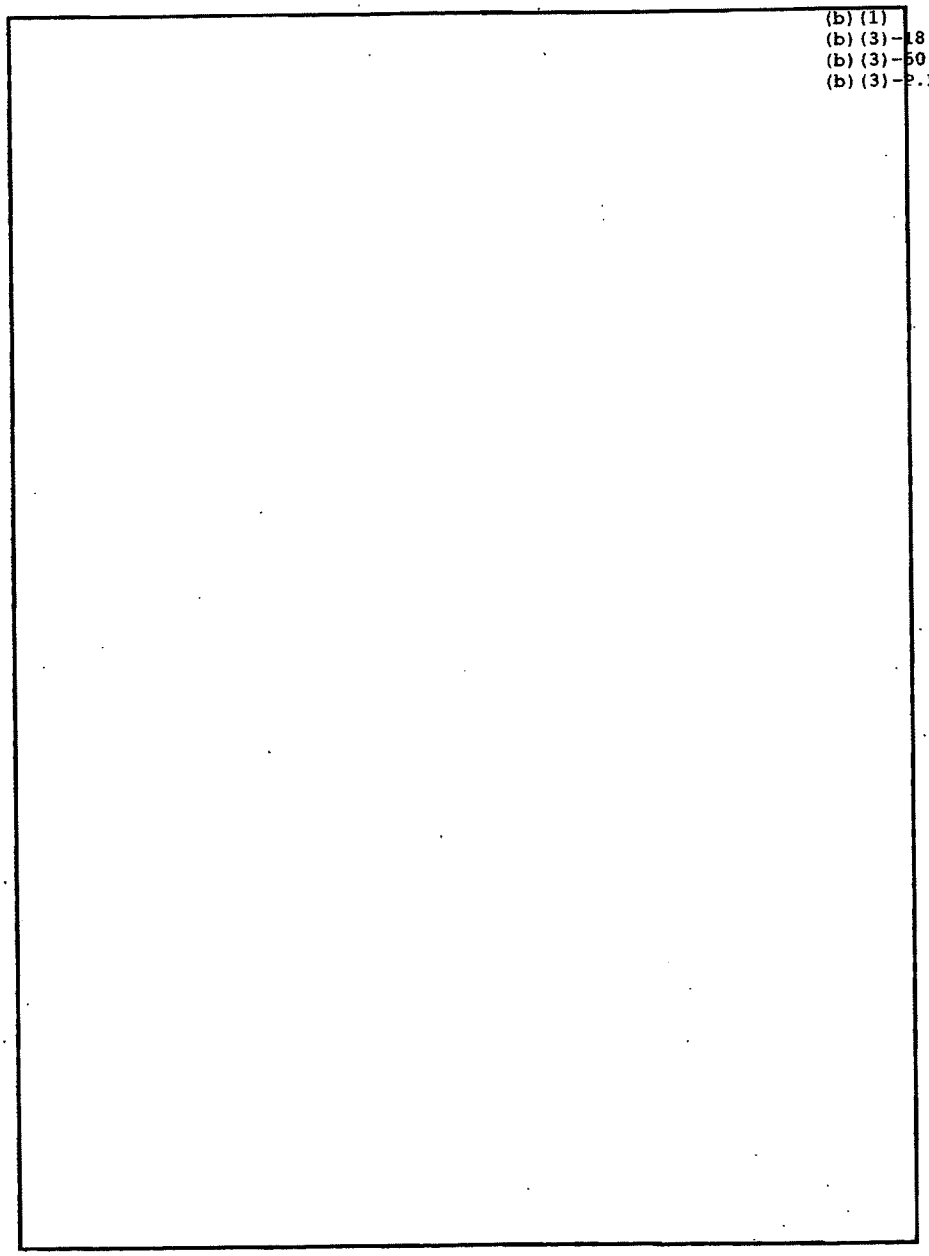
[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

5. **Collection of communications where sender and receiver are both within the United States**

- Collection of domestic communications would almost certainly fall within one of the definitions of electronic surveillance in FISA.
    - If the target of surveillance were a known US person inside the United States, it would fall within the first definition of electronic surveillance (1801(f)(1), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States.
    - If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance, irrespective of the "US-person" status of the communicants.
    - The intentional acquisition of purely domestic radio communications would fall within the third definition of electronic surveillance (f)(3), and a Court order would be required. However, as noted above and discussed in more detail below, domestic radio communications obtained unintentionally would not constitute a violation of the statute (though they must be destroyed upon recognition unless the Attorney General determined that the contents of the communication indicated s threat of death or serious bodily injury to any person).
    - Even if the first three definitions did not apply, the fourth definition (1801(f)(4)) would this activity if the means of collection required the installation or use of a surveillance device inside the United States to acquire the information (other than from a wire or radio communication) under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

FISA ISSUES
Paper Provided to HPSCI on March 28, 2006
Closed Hearing Held on March 29, 2006

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

I. FISA Issues

[redacted]

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123

[redacted]

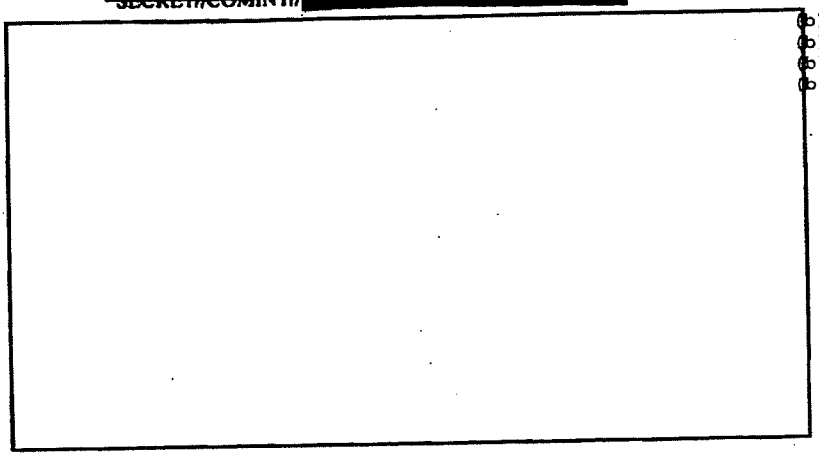
Other FISA issues

There are two major concerns with the language of the FISA, the first of which has already been discussed above to some degree. First, because of technological advances, the current jurisdiction of the FISC goes beyond the original intent of the statute. Second, the emergency provisions of FISA do not allow for a sufficiently rapid response to emergencies. Several other problems are also worthy of discussion.

1. Jurisdiction of the FISC

Many of the issues surrounding the FISA process concern the manner in which technological advances have in effect expanded the jurisdiction of the FISC. Realigning the jurisdiction of the Court to something that better approximates what FISA covered in practical terms in 1978 – providing protection for the privacy of communicants inside the United States -- would go a long way toward ameliorating many of the problems discussed herein.

[redacted]

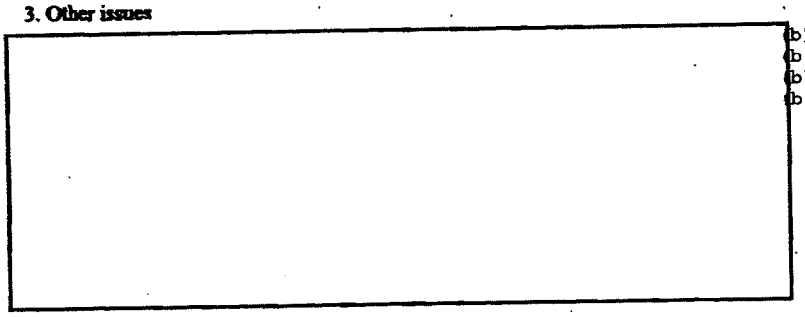


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

2. Emergencies

The Attorney General must approve emergency surveillances under FISA and the FISC must ratify his authorization within 72 hours. The problem is that the people who have the facts that provide the probable cause to justify the targeting are analysts at NSA (and CIA and FBI), and going to the Attorney General necessarily takes time. Realigning the jurisdiction of the FISC would free up more resources to work on emergencies, and, most importantly, there would be far fewer emergencies if the Attorney General did not have to approve targeting directed at non-US persons outside the US. Aside from that, the time required for emergency targeting could probably be cut down only by making the DOJ approval process less onerous (by allowing people below the Attorney General to make the authorization) or (even faster) by vesting the authority for authorization in the agencies who have the facts about the threat and requiring Attorney General/FISC ratification of the authorization after the fact.

3. Other issues



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

The FISA requires that the FISC be provided with a significant amount of information in requests that are submitted to it, and because the law also allows the Court to require "any additional information," many FISA applications now resemble finished intelligence products, rather than statements of probable cause with simple descriptions of how data will be collected and handled. The Court has also imposed requirements for submission of written descriptions of new collection techniques well in advance of applications employing them, as well as other additional reporting requirements, some of which go well beyond the purview of the judiciary (justification of the foreign intelligence value of what has been collected.) Meeting these requirements takes analysts and collectors from their primary jobs, and the need for them is questionable.

* * * * * * *

II. Responses to the five scenarios outlined by Chairman Hoekstra

The definitions of "electronic surveillance" in FISA require that one look at a number of factors to analyze the 5 scenarios described: the identity of the target, the location of the target, the type of communications being collected, and the location of collection. Thus, each of the scenarios has a variety of outcomes depending on how these factors are combined

1. **Collection of a communication between a point inside the United States and a point outside the United States if the collection occurs outside the United States**

   Under these circumstances:

- If the target of the surveillance were a US person inside the United States, the surveillance would fall within the first FISA definition of electronic surveillance (1801(f)(1)), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States. Therefore, a Court Order would be required.

- If the target of the surveillance were a non-US person outside the United States, none of the definitions of electronic surveillance in FISA would apply. Therefore, no Court Order would be required.

- If the target of the surveillance were a US person outside the United States, none of the definitions of electronic surveillance in FISA would apply. Therefore, no Court Order would be required. However, Attorney General approval would be required by E.O. 12333 to target such communications.

- If the target of the surveillance were a non-US person inside the United States, FISA would not apply, but Attorney General approval would ordinarily be required for the targeting if the means of communication was one in which this person would have a reasonable expectation of privacy. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

2. **Collection of a communication between a point inside the United States and a point outside the United States if the collection occurs inside the United States**

Under these circumstances:

- If the target of the surveillance were a US person inside the United States, the surveillance would fall within the first definition of electronic surveillance (1801(f)(1)), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States.
- If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance irrespective of the "US person" status of either communicant.
- If the target of the surveillance were a non-US person, or were a person outside the US, and the communication were collected while being transmitted by radio signal, FISA would not apply.
- If the communication were collected inside the United States by means other than intercept of a radio signal or collection from a wire or like connection, as above, FISA would still apply if the collection were effected through installation or use of some other surveillance device under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (e.g. installation and use of an implant on a computer within the United States).
- If the target of the surveillance were a US person outside the United States, FISA would not apply, but Attorney General approval would be required to do the targeting.
- If the target were a non-US person inside the United States, and NSA were seeking to intercept his international radio communications, FISA would not apply and no Court Order would be required. However, Attorney General approval would ordinarily be required for the targeting. [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

3. **Collection of a communication between a non-US person inside the United States and a point outside the United States, collection occurring anywhere**

Under these circumstances:

- If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance (1802(f)(2)), irrespective of the "US-person" status of the communicants.

- If the communication were being collected within the United States by means other than intercept of a radio signal or collection from a wire or like connection, FISA would still apply if the collection occurred through installation or use of some other surveillance device under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (e.g. installation and use of an implant on a computer within the United States) (see 1804(f)(4).

- If the communication were being collected outside the United States, or while being transmitted by radio signal (either within the United States or outside the United States), FISA would not apply, and no Court Order would be required.

- If the target were a US person outside the United States, FISA would not apply and no Court Order would be required. However, Attorney General approval would be required by E.O. 12333 to target such person's communications.

- If the target were a non-US person inside the United States, and NSA was seeking to intercept his international radio communications, FISA would not apply and no Court Order would be required. However, Attorney General approval would ordinarily be required to target such an individual's communications.

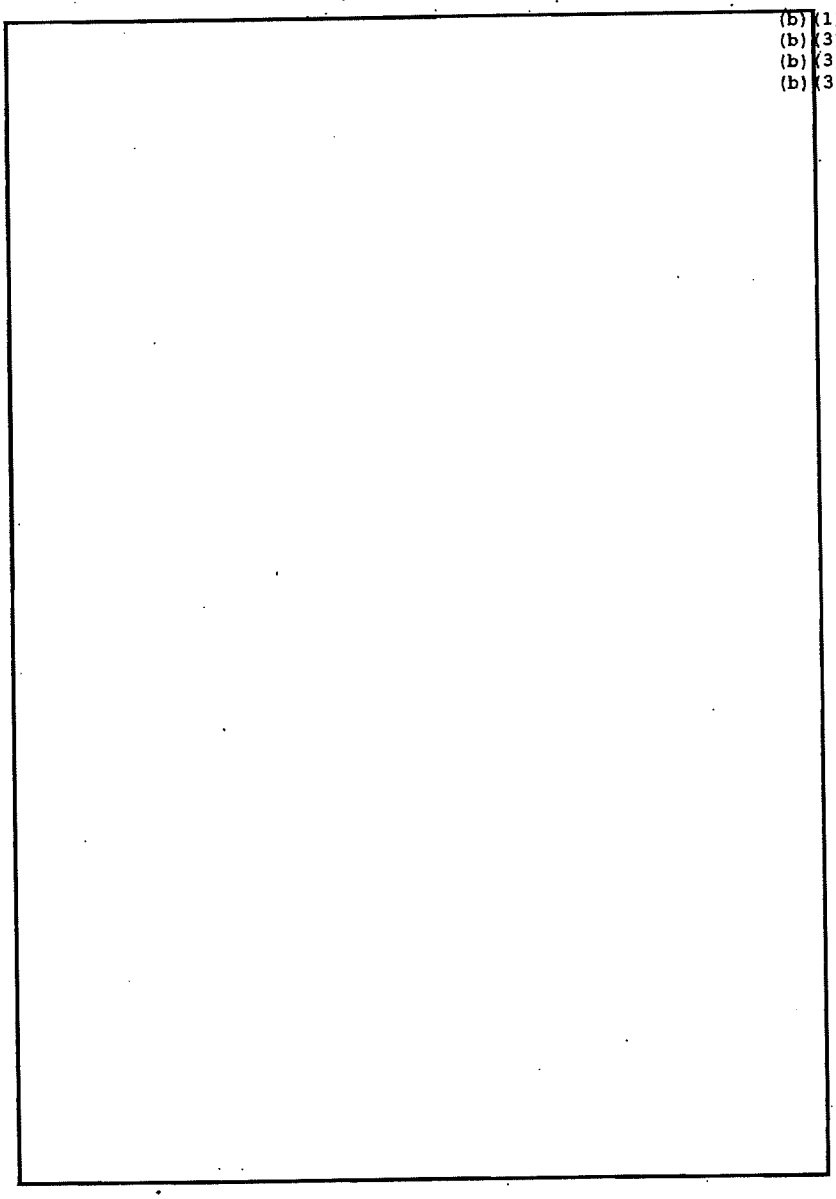
[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36



[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

5. Collection of communications where sender and receiver are both within the United States

- Collection of domestic communications would almost certainly fall within one of the definitions of electronic surveillance in FISA.
  - If the target of surveillance were a known US person inside the United States, it would fall within the first definition of electronic surveillance (1801(f)(1), which applies to the acquisition of radio or wire communications of a particular known US person who is in the United States.
  - If the communication were being collected while being transmitted on a wire or like connection within the United States, it would fall within the second definition of electronic surveillance, irrespective of the "US-person" status of the communicants.
  - The intentional acquisition of purely domestic radio communications would fall within the third definition of electronic surveillance (f)(3), and a Court order would be required. However, as noted above and discussed in more detail below, domestic radio communications obtained unintentionally would not constitute a violation of the statute (though they must be destroyed upon recognition unless the Attorney General determined that the contents of the communication indicated a threat of death or serious bodily injury to any person).
  - Even if the first three definitions did not apply, the fourth definition (1801(f)(4)) would this activity if the means of collection required the installation or use of a surveillance device inside the United States to acquire the information (other than from a wire or radio communication) under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.