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

December 10, 2007

Mr. John F. Hackett
Director, Information Management Office
Office of the Director of National Intelligence
Washington, DC 20511

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

Reference: DF-2007-00079
DF-2007-00080

Dear Ms. Hofmann:

This is a final response to your 31 August 2007 letters to the Office of the Director of National Intelligence, wherein you requested under the Freedom of Information Act (FOIA) the following information:

> **"...exchanges that Director McConnell or other ODNI officials have had with representatives of telecommunications companies concerning amendments to FISA..."**
>
> **"... exchanges that Director McConnell or other ODNI officials have had with members of the Senate or House of Representatives concerning amendments to FISA..."**

We processed your request in accordance with the FOIA, 5 U.S.C. § 552, as amended. Enclosed are 11 documents, totaling approximately 267 pages, that are responsive to your request. Upon review, it has been determined that portions of 29 pages should be withheld on the basis of FOIA Exemptions 1, 2 and 3, 5 U.S.C. § 552 (b)(1), (2), (3). In addition, 4 documents, totaling 14 pages, are being withheld in full on the basis of FOIA Exemptions 1, 3, 5 and 6, 5 U.S.C. § 552 (b)(1), (3), (5), (6), and because two of the documents are not agency records under the FOIA.

Pursuant to the Court's November 27, 2007 order, attached is a declaration setting forth the basis for the information being withheld. This declaration is provided to plaintiff without prejudice to ODNI's rights to provide additional information regarding the processing of plaintiff's FOIA requests and/or the reasons for any withholdings. ODNI specifically reserves the right to submit such additional information, as appropriate, in the context of summary judgment or other subsequent proceedings in this case.

Sincerely,

John F. Hackett

John F. Hackett
Director, Information Management Office

~~TOP SECRET~~//COMINT//COMPARTMENTED

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

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

MICHAEL DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

May 23, 2007

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

Dear Director McConnell:

I have had an opportunity to review the Administration's proposal to modernize the Foreign Intelligence Surveillance Act ("FISA") transmitted to the Committee on April 12, 2007. I have also reviewed the FISA Court orders dated [redacted] and the memoranda of law supporting them.

The Administration's proposal contains no special procedures to provide for electronic surveillance to be conducted following a terrorist attack or an armed attack on the United States. With these changes, will the system of obtaining warrants based on probable cause [redacted] in an individualized warrant be fast enough to protect the nation? Or, alternatively, does the Administration intend to continue to seek FISA Court approval for [redacted]

If the latter is the case, I believe the changes you have proposed to the statute do not specifically authorize these [redacted] warrants. I also do not believe the current statute envisions them, either. While we may disagree on this point, even the Attorney General has described the January orders as "innovative".

I strongly believe the FISA statute must be modernized so that we can listen to our enemies while protecting the civil liberties of Americans. But if Congress passes legislation that reaffirms that [redacted]

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

~~TOP SECRET//COMINT//COMPARTMENTED~~

I appreciate assistance from the Administration clarifying its intent on these matters and I look forward to working with you.

Sincerely,

Heather Wilson
Ranking Republican
Subcommittee on Technical
and Tactical Intelligence

cc: Attorney General Alberto Gonzales
Director Keith Alexander

(b)(1)
(b)(3)-P.L. 86-36

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

May 29, 2007

The Honorable Heather Wilson
Permanent Select Committee on Intelligence
House of Representatives
Washington, D.C. 20515

Dear Representative Wilson:

Thank you for your letter of May 23, 2007 commenting on the Administration's proposal to modernize the Foreign Intelligence Surveillance Act (FISA). I deeply appreciate your leadership role in this important effort.

As you observed, the Administration's proposal does not contain explicit procedures for conducting electronic surveillance following a terrorist attack. Such a provision was included in the bill (H.R. 5825) that you introduced last year. The Administration strongly supported H.R. 5825 and I welcome further discussions with you on this approach.

Under the Administration's proposal, in most cases, an order would not be required to target persons outside the United States. This provision was intended to grant the Intelligence Community the flexibility to collect the communications of non U.S. persons reasonably believed to be outside of the United States [redacted] However, the conduct of electronic surveillance targeted at U.S. persons inside the United States would generally remain within the scope of FISA.

[redacted] As you recognize, these issues involve innovative legal theories. We will, of course, advise you as these proceedings progress. To the extent FISA can be redrafted to address issues raised by the FISA Court, I would welcome such a statutory modification.

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

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

I look forward to meeting with you, at your earliest convenience, to further discuss this important matter. I appreciate your continued interest in modernizing FISA so that it will continue to serve the nation for years to come. Our most important duty is to do everything possible to protect America, while ensuring that we respect the Constitution, laws, and the civil liberties of all Americans in all of our activities.

Sincerely,

J.M. McConnell

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~HANDLE THROUGH CLASSIFIED CHANNELS~~

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

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

MICHAEL DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

September 24, 2007

The Honorable J. Michael McConnell
Director of National Intelligence
Washington, D.C. 20511

Dear Director McConnell:

During our September 20, 2007 hearing on the Foreign Intelligence Surveillance Act (FISA), you provided testimony concerning an incident in which three U.S. soldiers were kidnapped by Iraqi insurgents and the Administration subsequently obtained an emergency authorization from the Department of Justice to engage in electronic surveillance relating to the kidnapping. During your testimony, you noted that the surveillance was delayed for approximately 12 hours after the Administration identified targets for the surveillance. This Committee has been extensively briefed by the Intelligence Community on the details of this incident and received additional information from the National Security Agency (NSA) in the attached document.

Now that you have publicly discussed this incident, and given the number of recent press reports that contain erroneous and partial information about the reasons for the delay in beginning surveillance, I believe that it is important to clarify the reasons for the delay without revealing classified information. Therefore, I intend to release the following information, which I believe is an unclassified summary of the information we have received:

- On May 12, 2007, after a coordinated attack on their position south of Baghdad, three U.S. soldiers were reported missing and believed to have been captured by Iraqi insurgents. Immediately upon learning of the attack, theater-based and national SIGINT assets responded by dedicating all available resources to obtaining intelligence concerning the attack.

- On May 13 and 14, 2007, the Intelligence Community began to develop additional leads concerning the communications of insurgents claiming responsibility for the attack.

~~HANDLE THROUGH CLASSIFIED CHANNELS~~

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

- On May 15, 2007:
  - At 10:00 a.m., key U.S. agencies met to discuss and develop various options for collecting additional intelligence relating to the kidnapping by accessing communications [redacted]
  - At 10:52 a.m., the NSA notified [redacted] of its desire to collect some communications [redacted]
  - At 12:53 a.m., the NSA General Counsel agreed that all of the requirements for an emergency FISA authorization had been met for collection of the communications inside the U.S.
  - From 12:53 p.m. to 5:15 p.m., Administration lawyers and intelligence officials discussed the various legal and operational issues associated with the surveillance.
  - At 5:15 p.m., the Department of Justice's (DOJ) FISA office – the Office of Intelligence Policy and Review (OIPR) – received a call [redacted] formally requesting emergency authority to conduct the surveillance.
  - At 5:30 p.m., the OIPR attorney on duty attempted to reach the Solicitor General, who was the Acting Attorney General while Attorney General Gonzalez was addressing a United States Attorney's Conference in Texas. However, the Solicitor General had left for the day and was not able to authorize the emergency request. Eventually, a decision was made to attempt to reach Attorney General Gonzalez in Texas.
  - The OIPR attorney then contacted the Justice Department Command Center and requested that the Command Center locate the Attorney General in Texas. After several telephone calls with the staff accompanying the Attorney General, the OIPR lawyers were able to speak directly with the Attorney General and brief him on the facts of the emergency request.
  - At 7:18 p.m., the Attorney General authorized the requested surveillance. The Justice Department attorneys immediately notified the FBI.
  - At 7:28 p.m., the FBI notified key intelligence agencies and personnel of the approval.
  - At 7:38 p.m., surveillance began.

~~TOP SECRET//COMINT//20320108~~

~~HANDLE THROUGH CLASSIFIED CHANNELS~~

Should you have any concerns about the release of this information to the public, please notify me by 5:00 p.m. on Tuesday September 25, 2007.

Sincerely,

Silvestre Reyes
Chairman

~~HANDLE THROUGH CLASSIFIED CHANNELS~~

~~TOP SECRET//COMINT//20320108~~

(b)(1)
(b)(3)-P.L. 86-36

~~TOP SECRET//COMINT~~ [redacted] ~~ORCON//NOFORN//20320525~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE INTELLIGENCE STAFF
WASHINGTON, DC 20511

JUN 0 8 2007

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

The Honorable Peter Hoekstra
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Representative Hoekstra:

(U) Thank you for your May 31, 2007 letter to the Director of National Intelligence and the Attorney General. Director McConnell asked me to provide an interim response to your requests regarding the Committee's review of electronic surveillance activities. We are pleased that the Committee intends to consider the Administration's proposal to modernize the Foreign Intelligence Surveillance Act (FISA). We look forward to discussing with the Committee the critical national security need to update FISA to reflect current technology.

(U) We understand the Committee's desire to obtain certain documents relating to the President's Terrorist Surveillance Program and we will continue to work with you to address your needs. However, some of the documents requested by the Committee such as the President's authorizations of the Program are not within my discretion to provide. This is also the case with the Executive Branch legal opinions and any potentially responsive communications with the Foreign Intelligence Surveillance Court. These documents currently are the subject of an ongoing discussion within the Executive Branch.

(U) As you know, we have made every effort to provide the substance of the information that the Committee is seeking in this area. For instance, the Department of Justice (DoJ) has explained the legal reasoning underlying the Program in numerous hearings and briefings and would be happy to answer any remaining questions the Committee may have. The Committee has also been briefed on the President's authorizations. The Committee's particular request to have access to the January 2007 Foreign Intelligence Surveillance Court orders, applications, and exhibits filed in support of those applications has been accommodated by an agreement with DoJ.

DECL ON: 20320525
DRV FROM: [redacted]

~~TOP SECRET//COMINT~~ [redacted] ~~ORCON//NOFORN//20320525~~

(b)(1)
(b)(3)-P.L. 86-36

(U) Regarding the civil liberty safeguards of the Program, I understand that the National Security Agency (NSA) has briefed the Committee extensively on its applicable minimization procedures, as well as provided copies of relevant materials. In addition, NSA answered the Committee's questions about the rules for handling U.S. person information during recent briefings on the Program. As NSA has explained, the minimization procedures under the Program included NSA's Executive Order 12333 Attorney General Guidelines. The Attorney General approved these procedures for the collection, retention, and dissemination of information concerning U.S. persons in October 1982. The Secretary of Defense issued the current version of those procedures (DoD Regulation 5240.1-R) in December 1982. A classified annex to those procedures dealing specifically with signals intelligence was promulgated by the Deputy Secretary of Defense in April 1988 and approved by the Attorney General in May 1988. NSA internal procedures (USSID 18) were derived from those procedures and last updated in 1993. The annex that specifically governs FISA procedures was modified, with the Attorney General's approval, in 1997. NSA, of course, would be happy to provide additional briefings on this topic if the Committee desires, including how these rules apply to the Program.

(U) I also appreciate your interest in the effectiveness of the Program. In an effort to quantify its success, I have asked NSA to provide the Committee with a sample of the significant leads it has provided to the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), as it did for the Senate Select Committee on Intelligence (SSCI) and the Privacy and Civil Liberties Oversight Board.

(S//NF) [redacted] (b)(1)

(b)(1)
(b)(3)-P.L. 86-36

(TS//SI//[redacted]OC/NF) [redacted]

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

(U) We will continue to work with the Committee in response to your requests. In the meantime, I hope the Committee will give serious consideration to the Administration's proposal to modernize FISA. The proposal is being made thoughtfully, and after a year of extensive coordination and at the behest of Congress. It is critical that we work together to ensure that FISA will continue to serve the nation for years to come. Our most important duty is to do everything possible to protect America, while ensuring that we respect the Constitution, laws, and the civil liberties of all Americans in all of our activities.

(U) If you have any questions on this matter, please contact me or the Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted] (b)(2)

Sincerely,

Ronald L. Burgess, Jr.
Lieutenant General, USA

cc: The Honorable Alberto Gonzales
Lieutenant General Keith Alexander

- On May 12. 2007, after a coordinated attack on their position south of Baghdad, three U.S. soldiers were reported missing and believed to have been captured by Iraqi insurgents. Immediately upon learning of the attack, theater-based and national SIGINT assets responded by dedicating all available resources to obtaining intelligence concerning the attack.

- On May 13 and 14, 2007, the Intelligence Community began to develop additional leads concerning the communications of insurgents claiming responsibility for the attack, including approaching the FISA Court on May 14 for an amendment to a then-current order with some bearing on the hostage situation. The amendment was granted that day.

- As soon as specific leads had been identified, analysts began to compile all the necessary information to establish the factual basis for issuance of a FISA court order as required by the emergency authorization provision of the statute.

- On May 15, 2007:

    - At 10:00 a.m., key U.S. agencies met to discuss and develop various options for collecting additional intelligence relating to the kidnapping by accessing certain communications.

    - At 10:52 a.m., the NSA notified the Department of Justice (DOJ) of its desire to collect some communications that require a FISA order.

    - It was determined that some FISA coverage already existed.

    - At 12:53 p.m., the NSA General Counsel agreed that all of the requirements for an emergency FISA authorization had been met for the remaining collection of the communications inside the U.S.

    - From 12:53 p.m. to 5:15 p.m. Administration lawyers and intelligence officials discussed various legal and operational issues associated with the surveillance.

    - At 5:15 p.m, the DOJ's FISA office – the Office of Intelligence Policy and Review (OIPR) – received a call formally requesting emergency authority to conduct surveillance.

    - At 5:30 p.m., the OIPR attorney on duty attempted to reach the Solicitor General who was the Acting Attorney General while Attorney General Gonzales was addressing a United States Attorney's Conference in Texas. However, the Solicitor General had left for the day and the decision was made to attempt to reach Attorney General Gonzales in Texas.

    - The OIPR attorney then contacted the Justice Department Command

Center and requested that the Command Center locate the Attorney General in Texas. After several telephone calls with the staff accompanying the Attorney General, the OIPR lawyers were able to speak directly with the Attorney General and brief him on the facts of the emergency request.

- At 7:18 p.m., the Attorney General authorized the requested surveillance. The Justice Department attorneys immediately notified the FBI.

- At 7:28p.m, the FBI notified key intelligence agencies and personnel of the approval.

- At 7:38 p.m., surveillance began.

Sec. 401. **DEFINITION OF ELECTRONIC SURVEILLANCE.**

Subsection (f) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is amended by inserting after subsection (f)(4) the following:

"*Provided*, that nothing in this definition shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."

SEC. 402. AUTHORIZATION FOR THE ACQUISITION OF CERTAIN FOREIGN INTELLIGENCE INFORMATION.

Title I of the Foreign Intelligence Surveillance Act is amended by adding after section 102 (50 U.S.C. § 1802) the following:

''AUTHORIZATION FOR ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION

''SEC. 102A. (a) IN GENERAL.—Notwithstanding any other law, the President, acting through the Attorney General may, for periods of up to one year, authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that the Attorney General has determined that—

''(1) the acquisition does not constitute electronic surveillance;

''(2) the acquisition involves 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;

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

''(4) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

''(b) SPECIFIC PLACE NOT REQUIRED.—A certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

''(c) SUBMISSION OF CERTIFICATION.—The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of a certification made under subsection (a). Such certification shall be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless the certification is necessary to determine the legality of the acquisition under section 102B.

''(d) MINIMIZATION PROCEDURES.—An acquisition under this section may be conducted only in accordance with the certification of the Attorney General and the minimization procedures adopted by the Attorney General. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under section 108(a).

''DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE AND OTHER ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION

''SEC. 102B. (a) DIRECTIVE.—With respect to an authorization of an acquisition under section 102A, the Attorney General may direct a person to—

''(1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition of foreign intelligence information in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target; and

''(2) maintain under security procedures approved by the Attorney General and the Director of National

Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.

''(b) COMPENSATION.—The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (a).

''(c) FAILURE TO COMPLY.—In the case of a failure to comply with a directive issued pursuant to subsection (a), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (a) and is otherwise lawful. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

''(d) REVIEW OF PETITIONS.—(1) (A) A person receiving a directive issued pursuant to subsection (a) may challenge the legality of that directive by filing a petition with the pool established under section 103(e)(1).

''(B) The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges

serving in the pool established by section 103(e)(1). Not later than 48 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

''(2) A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply with such directive.

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

''(e) APPEALS.—The Government or a person receiving a directive reviewed pursuant to subsection (d) may file a petition with the Court of Review established under section 103(b) for review of the decision issued pursuant to subsection (d) not later than 7 days after the issuance of such decision. Such court of review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition for a writ of certiorari by the Government or any person receiving such directive, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

''(f) PROCEEDINGS.—Judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

''(g) SEALED PETITIONS.—All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

''(h) LIABILITY.—No cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

''(i) RETENTION OF DIRECTIVES AND ORDERS.—A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.''.

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

''102A. Authorization for acquisition of foreign intelligence information.

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

SEC. 403. TECHNICAL AMENDMENT AND CONFORMING AMENDMENTS.

Section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended--

(A) in paragraph (1), by striking ''501(f)(1)'' and inserting ''102B(d) or 501(f)(1)''; and

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

SEC. 404. EFFECTIVE DATE.

(a) Except as otherwise provided, the amendments made by this Act shall take effect immediately after the date of the enactment of this Act.

(b) Notwithstanding any other provision of this Act, any order in effect on the date of enactment of this Act issued pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall remain in effect until the date of expiration of such order, and, at the request of the applicant, the court established under section 103 (a) of such Act (50 U.S.C. 1803(a)) may reauthorize such order as long as the facts and circumstances continue to justify issuance of such order under the provisions of the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the applicable effective date of this Act. The court established under section 103(a) of such Act shall extinguish any such order at the request of the applicant.

SEC. 405. CLARIFICATION ON THE DEFINITION OF ELECTRONIC SURVEILLANCE.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is hereby amended by adding a new section 112 as follows:

"Section 112. Clarifications on the Definition of Electronic Surveillance. (1) Whenever a member of the Intelligence Community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a), as amended, intentionally acquires the communications of a non-U.S. person reasonably believed to be located outside the United States and the primary purpose of such acquisition to acquire the communications of a particular, known person reasonably believed to be located in the United States, such activities shall be considered "electronic surveillance" as defined in section 101(f)(1)."

Modernizing the Foreign Intelligence Surveillance Act

Statement for the Record

Senate Select Committee on Intelligence

June 21, 2007

J. Michael McConnell
Director of National Intelligence

Information as of
June 21, 2007

SENATE SELECT COMMITTEE ON INTELLIGENCE
FISA MODERNIZATION

CLASSIFIED

STATEMENT FOR THE RECORD

INTRODUCTION

Good morning Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee.

(U) I am pleased to be here today in my role as the head of the Intelligence Community (IC) to express my strong support for the legislation that will modernize the Foreign Intelligence Surveillance Act of 1978 (FISA). Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers and agents of foreign powers in the United States. My goal in appearing today is to share with you the critically important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the privacy rights of Americans.

(U) The proposed legislation to amend FISA has several key characteristics:

- It makes the statute technology-neutral. It seeks to bring FISA up-to-date with the changes in communications technology that have taken place since 1978;
- It seeks to restore FISA to its original focus on protecting the privacy interests of persons in the United States;
- It enhances the Government's authority to secure assistance by private entities, which is vital to the IC's intelligence efforts;
- And, it makes changes that will streamline the FISA process so that the IC can use FISA to gather foreign

intelligence information more quickly and efficiently.

(U) As the Committee is aware, I have spent the majority of my professional life in the IC. In that capacity, I have been both a collector and a consumer of intelligence information. I had the honor of serving as Director of the National Security Agency (NSA) from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function in enabling the collection of foreign intelligence information.

(U) In my first few months on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. I cannot overstate how instrumental FISA has been in helping the IC protect the nation from terrorist attacks since September 11, 2001.

~~(TS//SI//OC/NF)~~ Some of the specifics that support my testimony today cannot be discussed in open session. Accordingly, this classified statement contains additional, specific information concerning operational activities that demonstrate the need for FISA modernization. These include:

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

TODAY'S NATIONAL SECURITY THREATS

(U) Because I believe that the proposed legislation will advance our ability to protect the national security, I would like to take a few minutes to briefly discuss some of the current threats. The most obvious is the continued threat from international terrorists. Despite the fact that we are in the sixth year following the attacks of September 11, 2001, and despite the steady progress we have made in dismantling the al Qaeda organization, significant threats from al Qaeda, other terrorist organizations aligned with it, and its sympathizers remain.

(U) Today, however, America confronts a greater diversity of threats and challenges to attack inside our borders than ever before. As a result, the nation requires more from our IC than ever before.

(U) I served as the Director of NSA at a time when the IC was first adapting to the new threats brought about by the end of the

Cold War. Moreover, these new threats are enhanced by dramatic, global advances in telecommunications, transportation, technology, and new centers of economic growth.

(U) Although the aspects of Globalization are not themselves a threat, they facilitate terrorism, heighten the danger and spread of the proliferation of Weapons of Mass Destruction (WMD), and contribute to regional instability and reconfigurations of power and influence — especially through increasing competition for energy.

(U) Globalization also exposes the United States to complex counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded. Several non-state actors, including international terrorist groups, conduct intelligence activities as effectively as capable state intelligence services. Al Qaeda, and those aligned with and inspired by al Qaeda, continue to actively plot terrorist attacks against the United States, our interests and allies.

(U) A significant number of states also conduct economic espionage. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects approaching Cold War levels.

FISA NEEDS TO BE TECHNOLOGY-NEUTRAL

(U) In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs. Enacted nearly thirty years ago, it has not kept pace with 21st Century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S., i.e., foreign persons, located outside the United States. Currently, FISA forces a detailed examination of four questions:

- Who is the target of the communications?
- Where is the target located?
- How do we intercept the communications?
- Where do we intercept the communications?

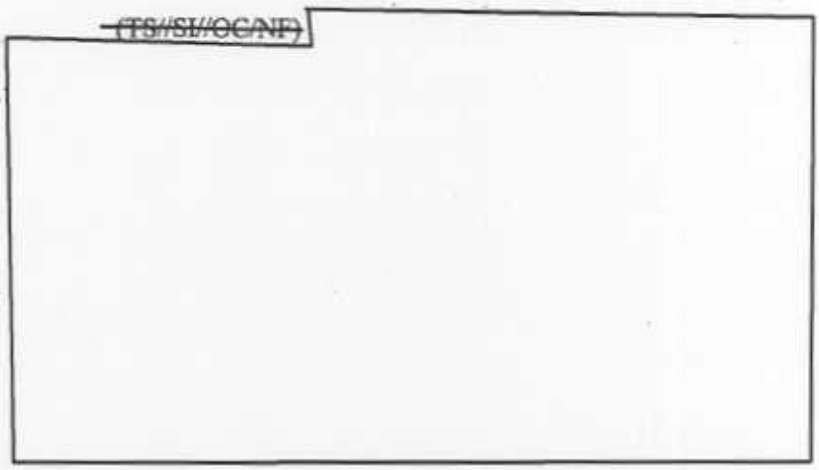
(U) This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

(U) FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and

collection out of the air.

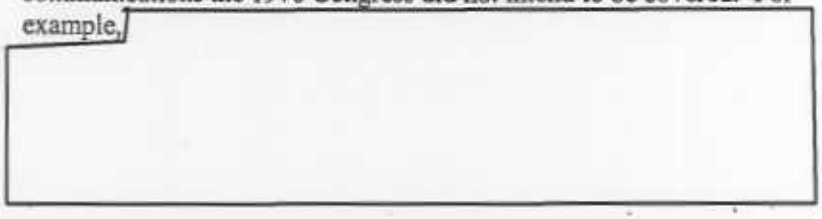
(U) Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

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



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

~~(TS//OC/NF)~~ Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications the 1978 Congress did not intend to be covered. For example,



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

~~(S//OC/NF)~~ In short, today communications currently fall under FISA that were originally excluded from the Act.

(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

(TS//SI//OC/NF)

(TS//SI//OC/NF)

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

(TS//SI//OC/NF)

In that circumstance, if U.S. person information were inadvertently collected, NSA followed the appropriate minimization procedures limiting acquisition, retention, and dissemination of the U.S. person information.

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

(TS//SI//OC/NF) I do want to be clear about one important point:

But, in some cases, a communication will go to a U.S. person That is not a new situation for NSA. NSA has been handling such a situation as part of its collections under E.O. 12333 and its minimization procedures for over 25 years.

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

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

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

~~(TS//SI//OC/NF)~~ The specific way the proposed FISA modernization legislation would remedy this is to allow U.S. intelligence greater access to foreign communications

(U) The solution is to make the FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what changes technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated or evolving technology.

~~(S)~~ Communications that, in 1978, would have been transmitted via radio or satellite, are transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, fiber optic cable transmissions currently fall under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

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

"the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

(U) Similarly, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

(U) And yet, simply because the law has not kept pace with our technology, communications intended to be excluded from FISA, are included. This has real consequences to the IC working to protect the nation from foreign threats.

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

(U) Today, IC agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the IC is often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas. Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause. This slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications that are significant to the national security.

~~(TS//SI//ORCON/NOFORN/FISA)~~ This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires.

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

[redacted] To state the case plainly: there are circumstances under which the government seeks to monitor, for purposes of protecting the nation from terrorist attack, the communications of foreign persons, who are physically located in foreign countries, the government is required under FISA to obtain a court order to authorize the collection. And we find ourselves in this

[redacted]

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

position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

(U) Moreover, this Committee and the American people should be confident that the information the IC is seeking is foreign intelligence information. Writ large, this includes information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States.

(U) While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that FISA's regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. It is important to note that nothing in the proposed legislation changes this basic premise in the law.

(U) Another thing that this proposed legislation does not do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States person. For example, during the course of its normal business under current law, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities. Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities that minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

(U) Some observers may be concerned about "reverse targeting" in which the target of the electronic surveillance is really a person in the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, FISA would require the IC —to seek approval from the FISA Court in order to undertake such electronic surveillance.

(U) In short, the FISA's definitions of "electronic surveillance" should be amended so that it no longer matters how collection occurs (whether off a wire or from the air). If the subject of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are

reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. If the government seeks to acquire communications of persons outside the United States, it will continue to be conducted under the lawful authority of Executive Order 12333, as it has been done for decades.

SECURING ASSISTANCE UNDER FISA

(U) The proposed legislation reflects that it is vitally important that the Government retain a means to secure the assistance of communications providers. As Director of NSA, a private sector consultant to the IC, and now Director of National Intelligence, I understand that in order to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

~~(TS//SI//OCANF)~~

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

This gives NSA the agility to detect possible terrorist threats against the United States in time to issue appropriate warnings.

(U) Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the government with the exercise of electronic surveillance that is subject to Court approval under FISA. However, as a result of the proposed changes to the definition of electronic surveillance, FISA does not provide a comparable mechanism with respect to authorized communications intelligence activities. The proposal would fill this gap by providing the Government with means to obtain the aid of a court to ensure private sector cooperation with lawful intelligence activities.

(U) This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private sector cooperation with activities that are "electronic surveillance" under current FISA, but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the IC in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA Modernization proposal contains a provision that would accomplish this objective.

THE FISA PROCESS SHOULD BE STREAMLINED

(U) In addition to updating the statute to accommodate new technologies, protecting the rights of people in the United States, and securing the assistance of private parties, the proposed legislation also makes needed administrative changes. These changes include:

(1) streamlining applications made to the FISA Court, and
(2) extending the time period the Department of Justice has to prepare applications following Attorney General authorized emergency collection of foreign intelligence information.

(U) The Department of Justice estimates that these process-oriented changes potentially could save thousands of attorney work hours, freeing up the Justice Department's National Security lawyers and the FISA Court to spend more of their time and energy on cases involving United States persons - - precisely the cases we want them to be spending their efforts on. And, if we combine the streamlining provisions of this bill with the technology-oriented changes proposed, the Intelligence Community will be able to focus its operational personnel where they are needed most.

FISA WILL CONTINUE TO PROTECT CIVIL LIBERTIES

(U) When discussing whether significant changes to FISA are appropriate, it is always appropriate to thoughtfully consider FISA's history. Indeed, the catalysts for FISA's enactment were abuses of electronic surveillance that were brought to light. The revelations of the Church and Pike committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving our intelligence capabilities. I want to emphasize to this Committee, and to the American people, that none of the changes being proposed are intended to, nor will have the effect of, disrupting the foundation of credibility and legitimacy that FISA established.

(U) Instead, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the Church and Pike investigations and the enactment of FISA. Following the adoption of FISA, a wide-ranging, new intelligence oversight structure was built into U.S. law. A series of laws and Executive Orders established oversight procedures and substantive limitations on intelligence activities. After FISA, the House and Senate each established intelligence oversight committees. Oversight mechanisms were established within the Department of Justice and within each intelligence agency – including a system of inspectors general.

(U) More recently, additional protections have been implemented community-wide. The Privacy and Civil Liberties Oversight Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. Unlike in the 1970s, the IC today operates within detailed, constitutionally-based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the

Executive Branch, and, through FISA, the judiciary.

(U) With this robust oversight structure in place, it is also important to also ensure that the IC is more effective in collecting and processing information to protect Americans from terrorism are other threats to the security of the United States. FISA must be updated to meet the new challenges faced by the IC.

(U) The Congressional Joint Inquiry Commission into IC Activities Before and After the Terrorist Attacks of September 11, 2001 recognized that there were systemic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and IC have continually sought ways to improve.

(U) The proposed changes to FISA address the problems noted by the Commission. At the same time, a concerted effort was made in our proposal to balance the country's need for foreign intelligence information with the need to protect core individual civil rights.

CONCLUSION

(U) This proposed legislation seeks to accomplish several goals:

(U) First, the changes proposed are intended to make FISA technology-neutral, so that as communications technology develops - - which it absolutely will - - the language of the statute does not become obsolete.

(U) Second, this proposal is not intended to change privacy protections for Americans. In particular, this proposal makes no changes to the findings required to determine that a U.S. person is acting as an agent of a foreign power. The proposal returns the FISA to its original intent of protecting the privacy of persons in the United States.

(U) Third, the proposed legislation enhances the Government's ability to obtain vital assistance of private entities.

(U) And fourth, the proposed legislation allows the Government to make some administrative changes to the way FISA applications are processed. As Congress has noted in its reviews of the FISA process, streamlining the FISA process makes for better government.

(U) This Committee should have confidence that we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully, and after extensive coordination for over a year.

(U) Finally, I would like to state clearly my belief that bipartisan support for bringing FISA into the 21st Century is essential. Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with Congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation. I ask for your support in modernizing FISA so that it will continue to serve the nation for years to come.

(U) As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's IC, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist activity and other threats to our security.

(U) I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st Century.

Modernizing the Foreign Intelligence Surveillance Act

Statement for the Record

Senate Select Committee on Intelligence

May 1, 2007

J. Michael McConnell
Director of National Intelligence

Information as of
May 1, 2007

SENATE SELECT COMMITTEE ON INTELLIGENCE
FISA MODERNIZATION

~~CLASSIFIED~~

STATEMENT FOR THE RECORD

INTRODUCTION

Good morning Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee.

(U) I am pleased to be here today in my role as the head of the Intelligence Community (IC) to express my strong support for the legislation that will modernize the Foreign Intelligence Surveillance Act of 1978 (FISA). Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers and agents of foreign powers in the United States. My goal in appearing today is to share with you the critically important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the privacy rights of Americans.

(U) The proposed legislation to amend FISA has several key characteristics:

- It makes the statute technology-neutral. It seeks to bring FISA up-to-date with the changes in communications technology that have taken place since 1978;
- It seeks to restore FISA to its original focus on protecting the privacy interests of persons in the United States;
- It enhances the Government's authority to secure assistance by private entities, which is vital to the IC's intelligence efforts;
- And, it makes changes that will streamline the FISA process so that the IC can use FISA to gather foreign

intelligence information more quickly and efficiently.

(U) As the Committee is aware, I have spent the majority of my professional life in the IC. In that capacity, I have been both a collector and a consumer of intelligence information. I had the honor of serving as Director of the National Security Agency (NSA) from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function in enabling the collection of foreign intelligence information.

(U) In my first eight weeks on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. I cannot overstate how instrumental FISA has been in helping the IC protect the nation from terrorist attacks since September 11, 2001.

~~(TS//SI//OC/NF)~~ Some of the specifics that support my testimony today cannot be discussed in open session. Accordingly, this classified statement contains additional, specific information concerning operational activities that demonstrate the need for FISA modernization. These include:

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

[redacted]

TODAY'S NATIONAL SECURITY THREATS

(U) Because I believe that the proposed legislation will advance our ability to protect the national security, I would like to take a few minutes to briefly discuss some of the current threats. The most obvious is the continued threat from international terrorists. Despite the fact that we are in the sixth year following the attacks of September 11, 2001, and despite the steady progress we have made in dismantling the al Qaeda organization, significant threats from al Qaeda, other terrorist organizations aligned with it, and its sympathizers remain.

(U) Today, however, America confronts a greater diversity of threats and challenges to attack inside our borders than ever before. As a result, the nation requires more from our IC than ever before.

(U) I served as the Director of NSA at a time when the IC was first adapting to the new threats brought about by the end of the

Cold War. Moreover, these new threats are enhanced by dramatic, global advances in telecommunications, transportation, technology, and new centers of economic growth.

(U) Although the aspects of Globalization are not themselves a threat, they facilitate terrorism, heighten the danger and spread of the proliferation of Weapons of Mass Destruction (WMD), and contribute to regional instability and reconfigurations of power and influence — especially through increasing competition for energy.

(U) Globalization also exposes the United States to complex counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded. Several non-state actors, including international terrorist groups, conduct intelligence activities as effectively as capable state intelligence services. Al Qaeda, and those aligned with and inspired by al Qaeda, continue to actively plot terrorist attacks against the United States, our interests and allies.

(U) A significant number of states also conduct economic espionage. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects approaching Cold War levels.

FISA NEEDS TO BE TECHNOLOGY-NEUTRAL

(U) In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs. Enacted nearly thirty years ago, it has not kept pace with 21st Century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S., i.e., foreign persons, located outside the United States. Currently, FISA forces a detailed examination of four questions:

- Who is the target of the communications?
- Where is the target located?
- How do we intercept the communications?
- Where do we intercept the communications?

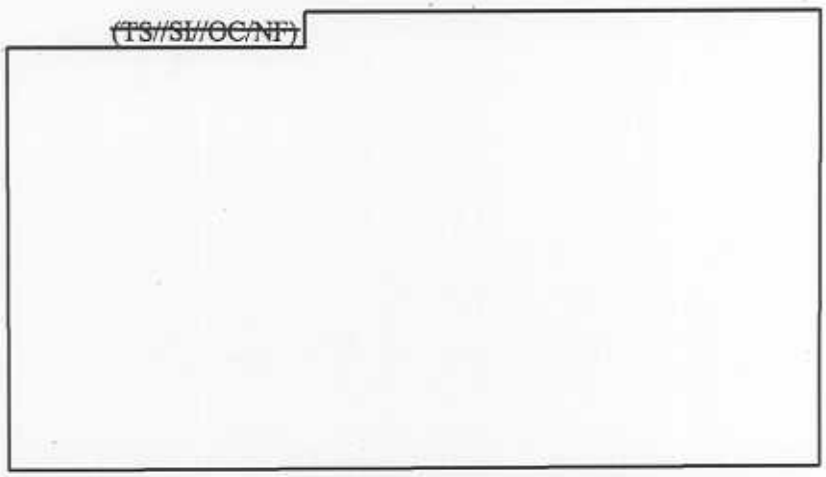
(U) This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

(U) FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and

collection out of the air.

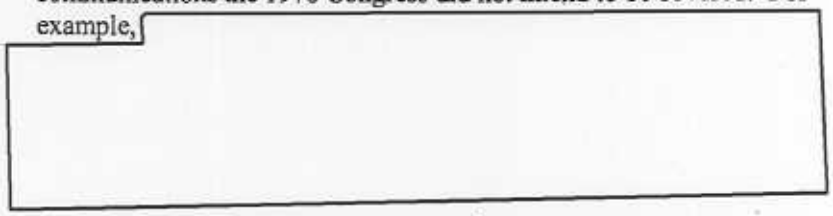
(U) Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

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



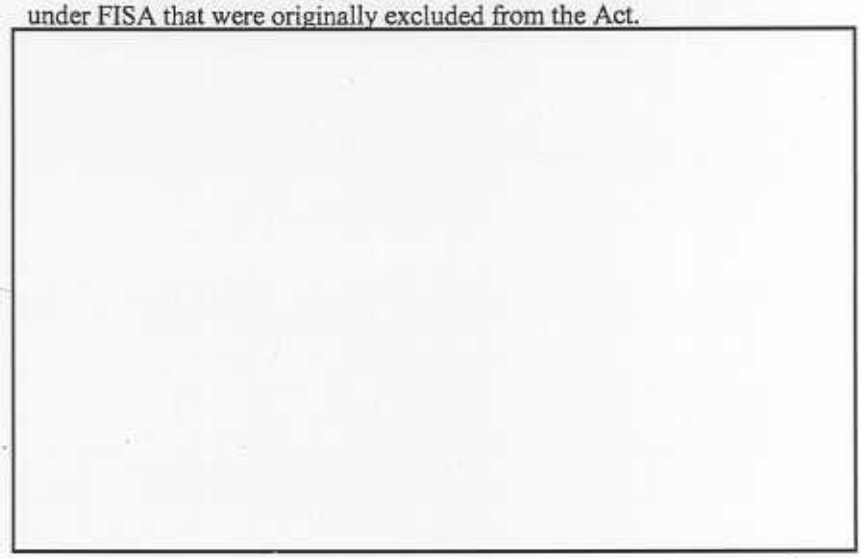
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~(TS//OC/NF)~~ Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications the 1978 Congress did not intend to be covered. For example,



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

~~(S//OC/NF)~~ In short, today communications currently fall under FISA that were originally excluded from the Act.



(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

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

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

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

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

In that circumstance, if U.S. person information were inadvertently collected, NSA followed the appropriate minimization procedures limiting acquisition, retention, and dissemination of the U.S. person information.

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

~~(TS//SI//OC/NF)~~ I do want to be clear about one important point:

But, in some cases, a communication will go to a U.S. person That is not a new situation for NSA. NSA has been handling such a situation as part of its collections under E.O. 12333 and its minimization procedures for over 25 years.

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

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

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

~~(TS//SI//OC/NF)~~ The specific way the proposed FISA modernization legislation would remedy this is to allow U.S. intelligence greater access to foreign communications

(U) The solution is to make the FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what changes technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated or evolving technology.

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

~~(S)~~ Communications that, in 1978, would have been transmitted via radio or satellite, are transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, fiber optic cable transmissions currently fall under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

"the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

(U) Similarly, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

(U) And yet, simply because the law has not kept pace with our technology, communications intended to be excluded from FISA, are included. This has real consequences to the IC working to protect the nation from foreign threats.

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

(U) Today, IC agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the IC is often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas. Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause. This slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications that are significant to the national security.

~~(TS//SI//ORCON/NOFORN/FISA)~~ This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires.

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

[redacted] To state the case plainly: there are circumstances under which the government seeks to monitor, for purposes of protecting the nation from terrorist attack, the communications of foreign persons, who are physically located in foreign countries, the government is required under FISA to obtain a court order to authorize the collection. And we find ourselves in this

[1] ~~(S)~~ [redacted]

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

position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

(U) Moreover, this Committee and the American people should be confident that the information the IC is seeking is foreign intelligence information. Writ large, this includes information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States.

(U) While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that FISA's regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. It is important to note that nothing in the proposed legislation changes this basic premise in the law.

(U) Another thing that this proposed legislation does not do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States person. For example, during the course of its normal business under current law, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities. Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities that minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

(U) Some observers may be concerned about "reverse targeting" in which the target of the electronic surveillance is really a person in the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, FISA would require the IC —to seek approval from the FISA Court in order to undertake such electronic surveillance.

(U) In short, the FISA's definitions of "electronic surveillance" should be amended so that it no longer matters how collection occurs (whether off a wire or from the air). If the subject of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are

reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. If the government seeks to acquire communications of persons outside the United States. it will continue to be conducted under the lawful authority of Executive Order 12333, as it has been done for decades.

SECURING ASSISTANCE UNDER FISA

(U) The proposed legislation reflects that it is vitally important that the Government retain a means to secure the assistance of communications providers. As Director of NSA, a private sector consultant to the IC, and now Director of National Intelligence, I understand that in order to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

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

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

This gives NSA the agility to detect possible terrorist threats against the United States in time to issue appropriate warnings.

(U) Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the government with the exercise of electronic surveillance that is subject to Court approval under FISA. However, as a result of the proposed changes to the definition of electronic surveillance, FISA does not provide a comparable mechanism with respect to authorized communications intelligence activities. The proposal would fill this gap by providing the Government with means to obtain the aid of a court to ensure private sector cooperation with lawful intelligence activities.

(U) This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private sector cooperation with activities that are "electronic surveillance" under current FISA, but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the IC in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA Modernization proposal contains a provision that would accomplish this objective.

THE FISA PROCESS SHOULD BE STREAMLINED

(U) In addition to updating the statute to accommodate new technologies, protecting the rights of people in the United States, and securing the assistance of private parties, the proposed legislation also makes needed administrative changes. These changes include:

(1) streamlining applications made to the FISA Court, and
(2) extending the time period the Department of Justice has to prepare applications following Attorney General authorized emergency collection of foreign intelligence information.

(U) The Department of Justice estimates that these process-oriented changes potentially could save thousands of attorney work hours, freeing up the Justice Department's National Security lawyers and the FISA Court to spend more of their time and energy on cases involving United States persons - - precisely the cases we want them to be spending their efforts on. And, if we combine the streamlining provisions of this bill with the technology-oriented changes proposed, the Intelligence Community will be able to focus its operational personnel where they are needed most.

FISA WILL CONTINUE TO PROTECT CIVIL LIBERTIES

(U) When discussing whether significant changes to FISA are appropriate, it is always appropriate to thoughtfully consider FISA's history. Indeed, the catalysts for FISA's enactment were abuses of electronic surveillance that were brought to light. The revelations of the Church and Pike committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving our intelligence capabilities. I want to emphasize to this Committee, and to the American people, that none of the changes being proposed are intended to, nor will have the effect of, disrupting the foundation of credibility and legitimacy that FISA established.

(U) Instead, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the Church and Pike investigations and the enactment of FISA. Following the adoption of FISA, a wide-ranging, new intelligence oversight structure was built into U.S. law. A series of laws and Executive Orders established oversight procedures and substantive limitations on intelligence activities. After FISA, the House and Senate each established intelligence oversight committees. Oversight mechanisms were established within the Department of Justice and within each intelligence agency – including a system of inspectors general.

(U) More recently, additional protections have been implemented community-wide. The Privacy and Civil Liberties Oversight Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. Unlike in the 1970s, the IC today operates within detailed, constitutionally-based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the

Executive Branch, and, through FISA, the judiciary.

(U) With this robust oversight structure in place, it is also important to also ensure that the IC is more effective in collecting and processing information to protect Americans from terrorism are other threats to the security of the United States. FISA must be updated to meet the new challenges faced by the IC.

(U) The Congressional Joint Inquiry Commission into IC Activities Before and After the Terrorist Attacks of September 11, 2001 recognized that there were systemic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and IC have continually sought ways to improve.

(U) The proposed changes to FISA address the problems noted by the Commission. At the same time, a concerted effort was made in our proposal to balance the country's need for foreign intelligence information with the need to protect core individual civil rights.

CONCLUSION

(U) This proposed legislation seeks to accomplish several goals:

(U) First, the changes proposed are intended to make FISA technology-neutral, so that as communications technology develops - - which it absolutely will - - the language of the statute does not become obsolete.

(U) Second, this proposal is not intended to change privacy protections for Americans. In particular, this proposal makes no changes to the findings required to determine that a U.S. person is acting as an agent of a foreign power. The proposal returns the FISA to its original intent of protecting the privacy of persons in the United States.

(U) Third, the proposed legislation enhances the Government's ability to obtain vital assistance of private entities.

(U) And fourth, the proposed legislation allows the Government to make some administrative changes to the way FISA applications are processed. As Congress has noted in its reviews of the FISA process, streamlining the FISA process makes for better government.

(U) This Committee should have confidence that we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully, and after extensive coordination for over a year.

(U) Finally, I would like to state clearly my belief that bipartisan support for bringing FISA into the 21st Century is essential. Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with Congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation. I ask for your support in modernizing FISA so that it will continue to serve the nation for years to come.

(U) As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's IC, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist activity and other threats to our security.

(U) I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st Century.

Summary of [redacted] Electronic Surveillance Coverage

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, in addition to other members of Congress, have been briefed on [redacted] electronic surveillance coverage of important terrorist and other targets currently faced by the Intelligence Community. This paper provides a summary [redacted] The situation is exceedingly fluid and new collection opportunities arise daily. [redacted] We are available to brief Members of Congress in greater detail.

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

(U//~~FOUO~~) The Foreign Intelligence Surveillance Act (FISA), enacted in 1978 in a time of simpler technology, was not designed to keep up with rapidly changing non-state threats in today's digital environment. This has direct consequences to the Intelligence Community's ability to protect the nation from foreign threats.

~~(TS//SI//NF)~~ [redacted] For example, FISA often requires the Government to make a showing of probable cause and obtain FISA Court approval when targeting a foreign person overseas [redacted]

~~(TS//SI//NF)~~ [redacted] the FISA court requires extensive probable cause justifications [redacted]

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

[1] ~~(TS//SI//NF)~~ [redacted]

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

Unlike earlier documentation that was readily understood by intelligence professionals, FISA court documents require agencies to go into extensive detailed explanations that can be understood by non-intelligence professionals.

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

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

Our strongest recommendation, of course, is that the IC should not be required to obtained FISA Court orders to collect the communications of foreign persons reasonably believed to be located outside the United State regardless of the communications mode, i.e., wire or radio based.

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

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

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

(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

(U//~~FOUO~~) This is not an acceptable situation. We call upon you to enact the Administration's request to modify the FISA before the August recess.

Attachment 1

(U) QUESTION: Under the Protect America Act, if the U.S. government decides to target all the communications of a particular foreign company, for any foreign intelligence purpose, and that foreign company has regular communications with a company in the United States, all of the calls and emails that the employees of the U.S. company exchange with the foreign company could be monitored, with no requirement to ever get a warrant, and no legal requirement that the calls or emails be linked to terrorism or a specific threat against the United States. Is this correct?

~~(S//SI//NF)~~ ANSWER: Decisions about which foreign targets should be subject to surveillance for foreign intelligence purposes are made by professional intelligence officers who are experts in their fields. Relying upon the best available intelligence and subject to appropriate and vigorous oversight, [redacted] because of the analyst's best judgment that the interception of its communications will result in the collection of foreign intelligence information that is responsive to documented intelligence requirements.

~~(S//SI//NF)~~ Assuming that valid foreign intelligence is expected to be obtained by targeting the foreign [redacted] mechanisms are in place to ensure that the Fourth Amendment rights of any U.S. person communicating with the foreign [redacted] are protected. Any incidentally collected information to, from, or about a person in the United States would be handled in accordance with the relevant minimization procedures. Such procedures – issued pursuant to Executive Order 12333, approved by the Attorney General, and shared with the intelligence committees – have served over decades as both a reliable and practical method of ensuring the constitutional reasonableness of the National Security Agency's (NSA) collection activities under Executive Order 12333. In addition, under the Protect America Act, the National Security Agency (NSA) is using minimization procedures previously approved by the FISA Court.

~~(U//FOUO)~~ If the collection does not contain foreign intelligence, no dissemination takes place and the data "ages off" the system. If the collection contains foreign intelligence, the information is subjected to appropriate minimization procedures. (A detailed explanation of NSA's minimization process is attached.)

(U) Attachment 2: NSA'S Minimization Procedures

(U) NSA's minimization procedures are an important way the Agency protects the privacy rights of Americans. This paper explains what they require and how NSA applies them. This paper also discusses the procedures required by the Protect America Act of 2007 to determine whether the subject of surveillance is reasonably believed to be located outside the United States.

~~(C//REL USA, FVEY)~~ *What is minimization?* NSA collects foreign intelligence information to meet documented intelligence requirements. This collection effort is primarily focused on targets located outside the United States. The bulk of NSA intelligence reporting does not include information about U.S. persons. In the event NSA collects information to, from, or about a U.S. person, the Agency has in place a set of procedures to ensure that privacy rights of persons in the United States are protected under the Fourth Amendment. These "minimization" procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. It is more than just the masking of U.S. person identities (i.e., obscuring so as not to identify or contextually identify). Minimization safeguards U.S. persons' rights by closely regulating the conduct of electronic surveillance that may result in the acquisition of information regarding U.S. persons.

(U) *Where does the need for minimization procedures come from?* The most direct answer is Executive Order 12333. Section 2.3 of that Order specifies that agencies in the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. In NSA's case, the Secretary of Defense has issued these required procedures as DoD Regulation 5240.1-R and its classified annex. They have been approved by the Attorney General and provided to the Intelligence Committees. NSA summarized these and other related procedures as "Legal Compliance and Minimization Procedures," an internal document often referred to as "USSID SP0018," or "U.S. Signals Intelligence Directive 18."

(U) *How does NSA acquire information about U.S. persons?* Broadly speaking, NSA acquires information about U.S. persons in one of two ways.

a. NSA may only target a U.S. person directly if there is reason to believe that person to be a foreign power or agent of a foreign power.

--If that U.S. person is overseas and a warrant would be required for law enforcement purposes, NSA is required under Executive Order 12333 (section 2.5) to obtain authorization from the Attorney General. NSA must demonstrate, and the Attorney General must agree, that there is probable cause to believe that the NSA collection is directed against a foreign power or agent of a foreign power.

~~Derived From: NSA/CSS [illegible]~~
~~[illegible]20070108~~
Declassify On: 20320108

--If that person is in the United States, NSA must obtain an order from the FISA Court, likewise premised on a finding that the U.S. person is an agent of a foreign power.

b. NSA may unintentionally obtain information about a U.S. person. This "incidental" collection occurs when NSA targets a foreigner overseas and, in so doing, collects information to, from, or about a U.S. person. Member and staff questions have centered around this form of collection, so the remainder of this document will focus on these questions.

(b)(3)-P.L. 86-36

~~(U//FOUO)~~

~~(S//SI//REL USA, FVEY)~~ *What does NSA do with incidentally acquired U.S. person information*? As discussed in the unclassified paper, the key issue is whether the information NSA acquires constitutes foreign intelligence.[1] If so, NSA analysts will disseminate it to a range of intelligence customers that have levied intelligence requirements about the target. If it is not foreign intelligence, NSA does not disseminate it for intelligence purposes. While not an exact science, analysts over time develop an excellent working knowledge of their targets [redacted] This, combined with a working knowledge of intelligence requirements, informs an analyst's judgment about what constitutes foreign intelligence.

(U) *Are there instances when NSA may reveal the identity of a U.S. person without waiting to be asked by a customer*? Yes. NSA's minimization procedures permit the Agency to disseminate the U.S. person's identity when it is required to understand or assess the foreign intelligence. For example, when the identity is pertinent to the safety of a person or entity or when the target, i.e., a U.S. person overseas, is the subject of surveillance authorized by the Attorney General under E.O. 12333 section 2.5. NSA has established a process, including senior level review prior to release of the information.

(b)(3)-P.L. 86-36

~~(U//FOUO)~~ ~~(U)~~ *When NSA is acquiring the communications of a person in the United States during its targeting of a foreigner overseas, is it reasonable to impose a time limit on NSA's determination of whether to target the person in the United States or drop that individual?* It is not reasonable to impose time limits on NSA's targeting determinations in this manner. If frequent contacts occur between the foreign target overseas and a person in the United States and if there is no foreign intelligence to be obtained, analysts will [redacted] such that the interception of the communications of the person in the United States when targeting the foreigner overseas will not occur. If valid collection of the foreign intelligence target indicates that the person in the United States is of intelligence interest, NSA would disseminate an intelligence report with the identity masked to the FBI, which could seek a FISA Court order to conduct electronic surveillance in the United States. If valid foreign intelligence is expected to be obtained by targeting the foreign selector, any incidentally collected information about the person in the United States would be handled in accordance with NSA's minimization procedures.

(U) *Would NSA object to a legislative codification of E.O. 12333 minimization procedures?* Yes because it can be difficult to change a statute if the procedures need to be changed in order to meet operational needs.

[1] Foreign intelligence is defined in USSID 18 as including information relating to the capabilities, intentions, and activities of foreign powers, organization, or persons.

~~(S//SI//REL USA, FVEY)~~ *There is a provision in USSID 18 that requires an annual NSA review* [redacted] *(USSID SP0018 section 5.2). According to that provision, the purpose of the review shall be to determine whether there is reason to believe that foreign intelligence will be obtained, or will continue to be obtained,* [redacted] *Because NSA is required to conduct this review, could USSID SP0018 section 5.2 form the basis of a legislative provision requiring a FISA Court order* [redacted] No. On the surface, one might think that NSA first determines [redacted] However, that is not the case. It is very difficult, if not impossible, [redacted] to determine whether or not there is reason to believe that foreign intelligence will be obtained. [redacted]

~~(S//SI//REL USA, FVEY)~~ Any legislative provision along the suggested lines would essentially force NSA to [redacted] to make a radical and extraordinarily inefficient change to the way its analysts process intercept. [redacted]

~~(S//SI//REL USA, FVEY)~~ More significantly, asking a judge to make a determination as to whether there is reason to believe that [redacted] strategy will result in the acquisition of foreign intelligence would require analysts to formally describe in great detail the reasoning behind all of their targeting of non-U.S. persons outside the United States. NSA's experience in providing the FISA Court with probable cause to believe that [redacted] is tied to a terrorist group has demonstrated that it is more often than not an extraordinarily time-consuming process. [redacted]

~~(S//SI//REL USA, FVEY)~~ *How many times has NSA obtained a FISA order to target a person in the United States where the initial target was a foreigner overseas and a U.S. communicant became of foreign intelligence interest? How many cases have there been where the target remains the foreigner overseas and there have been multiple communications between that target and a person in the United States such that NSA considered whether to obtain a FISA order to conduct electronic surveillance against the person in the United States?* This is difficult to answer because NSA routinely provides information to the FBI and it decides whether to follow up by getting a FISA order to conduct electronic surveillance in the United States. For example, if an analyst reviews an intercept and finds evidence that a party to the communication (not the target of the surveillance) is a U.S. person, he would go through his foreign intelligence calculus. That is, he determines whether the communication contains foreign intelligence. If he

determines that it does contain foreign intelligence, he would disseminate a foreign intelligence report. The report would mask the U.S. person's identity as "U.S. person" under NSA's minimization procedures. Upon receipt, a customer (here probably the FBI) would likely request that person's identity. Under NSA's minimization procedures, NSA would provide it if the requester demonstrates that the request is within the scope of its mission and knowing the U.S. person's identity is necessary to understand or assess the foreign intelligence in the report. In this case, the FBI would likely meet that test and, upon receipt of the identity, can decide whether or not to follow up. NSA surveillance against the foreign target would continue.

~~(S//REL USA, FVEY)~~ *What minimization procedures is NSA using under the Protect America Act*? Under the Protect America Act, NSA is using minimization procedures previously approved by the FISA Court.

~~(S//SI//REL USA, FVEY)~~ *What procedures does NSA have under the Protect America Act to determine whether the target of the surveillance is reasonably believed to be outside the United States?* Under the Protect America Act, NSA determines whether a person is reasonably believed to be outside the United States based on the totality of information available with respect to that person.

[redacted]

After [redacted] has been vetted by the analyst through the above processes, it then goes through serial reviews by various levels of supervisory personnel to ensure any inadvertent mistakes are prevented.

~~(TS//SI//NF)~~ It is important to note that while NSA can ensure that there is a basis to reasonably believe that [redacted] is outside the United States, it cannot ensure that all communicants in communication with [redacted] are outside the United States, as it is impossible to anticipate who will communicate with the target. For this reason, when the communicant with the target is a U.S. person, NSA applies the above-described minimization procedures, in a manner analogous to its handling of U.S. person information encountered when it targets foreign communications under its traditional E.O. 12333 authorities.

~~(TS//SI//NF)~~ The process does not end when [redacted] is tasked, as the analyst is required to continually examine [redacted] NSA judges that the above-referenced procedures are extremely effective in ensuring that the targeted communications are outside the United States. [redacted]

~~(S//SI//REL USA, FVEY)~~ *How does NSA assure compliance with the "foreign-ness" procedures under the Protect America Act*? Pursuant to its implementation of the Protect America Act, NSA has established extensive compliance mechanisms, which ensure [redacted] that all tasking is performed according to all approved procedures and that raw traffic is labeled and stored only in authorized repositories. Analysts receive training and are tested on their understanding of the procedures. (Note that this training is in addition to regular USSID 18 training.) There are serial reviews by various levels of supervisory personnel to ensure that inadvertent mistakes are caught and measures are implemented to prevent recurrence. There is continued oversight and periodic reviews by NSA's SIGINT Directorate Office of Oversight and Compliance, Office of Inspector General, and Office of General Counsel, as well as by the Department of Justice and the Office of the Director of National Intelligence. The implementation process also includes the creation, tracking, and reporting to Congress of performance metrics, which quantitatively and qualitatively measure our success in fulfilling our mission as well as our compliance with our internal controls and procedures. In that regard, we have already conducted numerous briefings and onsite visits with members of the House and Senate Intelligence and Judiciary Committees describing our implementation status and processes to date. We have also provided the Intelligence Committees with copies of the DNI/Attorney General certifications under the Protect America Act with attachments.

(U) Attachment 3: NSA'S Minimization Procedures

~~(U//FOUO)~~ NSA **collects foreign intelligence information** to meet documented intelligence requirements.

- ~~(U//FOUO)~~ This collection effort is **primarily focused on targets located outside the United States**. The bulk of NSA intelligence reporting **does not include information about U.S. persons**.

- ~~(U//FOUO)~~ In the event NSA collects information to, from, or about a U.S. person, the Agency has in place a set of procedures to ensure that **privacy rights of persons in the United States are protected under the Fourth Amendment.** These "minimization" procedures govern the **entire process** NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information.

~~(U//FOUO)~~ Here is how the minimization process works when NSA produces an intelligence report:

- ~~(U//FOUO)~~ **To Include in Report or Not?** Once the analyst has determined that the collection contains foreign intelligence, the analyst next determines whether the U.S. person's involvement is critical to understanding the foreign intelligence. If it is not, then even the fact that a U.S. person is involved will not be included in any foreign intelligence reporting.

- ~~(U//FOUO)~~ **To Include.** If the U.S. person's involvement is essential to understanding the foreign intelligence, the analyst will ordinarily mask the identity so that the reader cannot identify the U.S. person. Examples of generic masking include: "U.S. person," "U.S. company," or "U.S. official."

- ~~(U//FOUO)~~ **To Identify**. NSA customers may request a U.S. identity that has been masked if their official duties require the U.S. identify in order to understand or assess the foreign intelligence. A senior NSA official will review the report and the justification for requesting the identity, make a decision to approve or deny release, and document that release.

- ~~(U//FOUO)~~ **Exceptions.** NSA's minimization procedures describe a limited number of situations in which U.S. identities may be included unmasked in SIGINT reporting. These situations, including situations of threat to safety, are described in procedures that include appropriate levels of approval for releasing the identity in the report.