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.

~~DECLASSIFY 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?

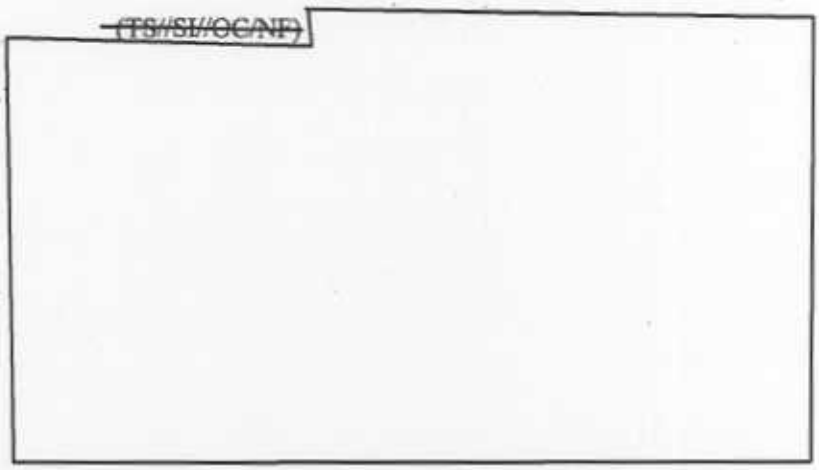
(U) This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

(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.

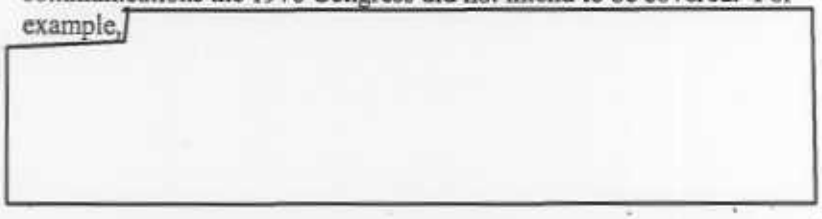
(U) Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

~~(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?

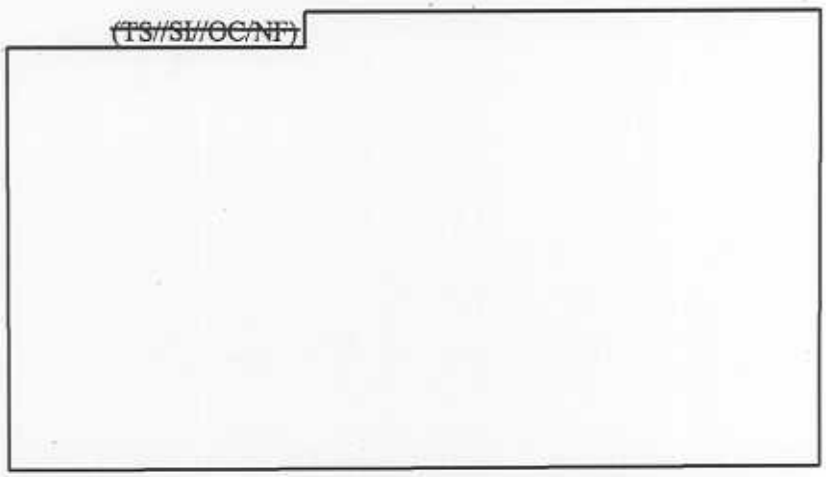
(U) This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

(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.

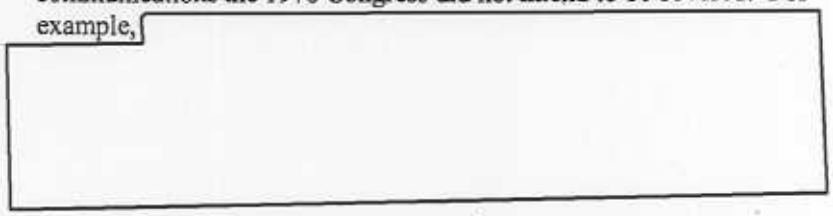
(U) Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

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



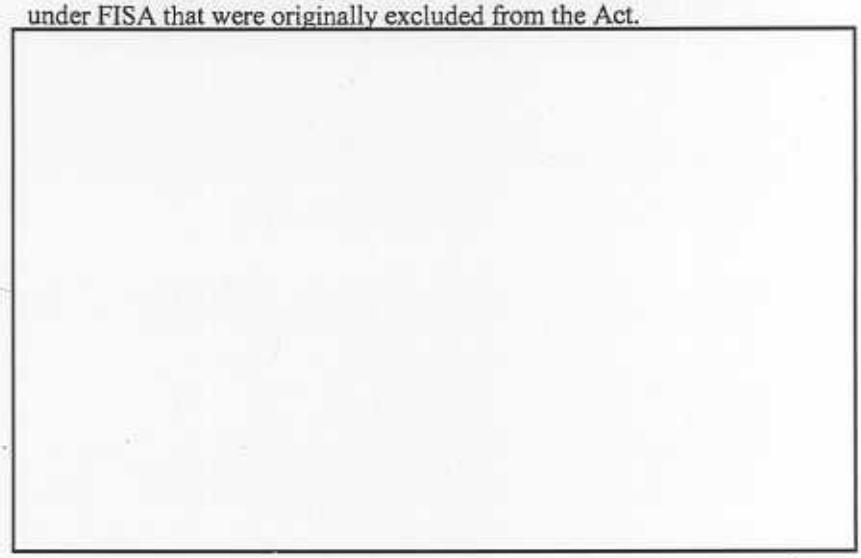
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~(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.

A Bill

To authorize appropriations for fiscal year 2008 for intelligence and intelligence-related activities of the United States Government and the Office of the Director of National Intelligence, the Central Intelligence Agency Retirement and Disability System, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SEC. 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Authorization Act for Fiscal Year 2008".

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

## TITLE I - INTELLIGENCE ACTIVITIES.

### Subtitle A. General Provisions.

**SEC. 101. AUTHORIZATION OF APPROPRIATIONS.**

Funds are hereby authorized to be appropriated for fiscal year 2008 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

(1) The Office of the Director of National Intelligence.

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

(6) The Department of the Army, the Department of the Navy, and the Department of the Air Force.

(7) The Coast Guard.

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Federal Bureau of Investigation.

(12) The Drug Enforcement Administration.

(13) The National Reconnaissance Office.

(14) The National Geospatial-Intelligence Agency.

(15) The Department of Justice.

(16) The Department of Homeland Security.

**SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.**

(a) SPECIFICATIONS OF AMOUNTS AND PERSONNEL CEILINGS.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence and intelligence-related activities of the elements listed in such section are those specified in the classified Schedule of Authorizations prepared to accompany the conference report on the bill _____ of the One Hundred Tenth Congress.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—The Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President. The President shall provide for suitable distribution of the Schedule, or of appropriate portions of the Schedule, within the Executive Branch.

**SEC. 103. ELIMINATION OF CERTAIN PERSONNEL MANAGEMENT CONSTRAINTS.**

The National Security Act of 1947 is amended by adding a new paragraph (s) to Section 102A:

(s) RELIEF FROM CIVILIAN END STRENGTH CEILINGS. (1) The personnel of elements of the Intelligence Community, as defined by section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)), as amended, shall be managed each fiscal year solely on the basis of and consistent with -

(A) the workload required to carry out authorized functions and activities, and

(B) the funds made available to elements of the Intelligence Community for such fiscal year.

(2) The management of such personnel in any fiscal year shall not be subject to any constraint or limitation in terms of man years, end strength, full-time equivalent positions, or maximum number of employees. The Director of National Intelligence, the Director of the Central Intelligence Agency, and the head of the department or agency containing elements of the Intelligence Community may not be required to make a reduction in the number of full-time equivalent positions in an element of the Intelligence Community unless such reduction is necessary due to a reduction in funds available to that element of

the Intelligence Community, or is required under a law, that is enacted after the date of enactment of this Act, and that refers specifically to this subsection.

(3) In order to ensure appropriate oversight, the Director of National Intelligence, in consultation with the head of each department or agency which contains an element of the Intelligence Community, shall submit, as part of the President’s annual budget, a projection of employment levels based on mission requirements, workload, and other considerations.

**SEC. 104. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.**

The authorization of appropriations by this Act shall not be deemed to constitute authority for the conduct of any intelligence activity which is not otherwise authorized by the Constitution or the laws of the United States.

**SEC. 105. DEFINITION OF INTELLIGENCE COMMUNITY.**

Section 3(4)(L) of the National Security Act of 1947 (50 U.S.C. 401a(4)(L)), as amended by section 1073 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended by striking “other” the second time it appears.

**SEC. 106. ADDITIONAL ADMINISTRATIVE AUTHORITY OF THE DIRECTOR OF NATIONAL INTELLIGENCE.**

Section 102A of the National Security Act of 1947 (50 U.S.C. 403–1) is amended by adding at the end the following new subsections:

‘‘(s) ADDITIONAL ADMINISTRATIVE AUTHORITIES.—

(1) Notwithstanding section 1346 of title 31, United States Code, or any other provision of law prohibiting the interagency financing of activities described in subparagraphs (A) or (B), upon the request of the Director of National Intelligence, elements of the Intelligence Community are authorized to use appropriated funds to support or participate in the following interagency activities of the Intelligence Community:

‘‘(A) national intelligence centers established by the Director under section 119B; and

‘‘(B) boards, commissions, councils, committees, and similar groups established by the Director for a period not to exceed two years.

‘‘(2) No provision of law enacted after the date of the enactment of this subsection shall be deemed to limit or supersede the authority in paragraph (1) unless such provision makes specific reference to the authority in that paragraph.

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

**SEC. 108. EXTENSION TO THE INTELLIGENCE COMMUNITY OF AUTHORITY TO DELETE INFORMATION ABOUT RECEIPT AND DISPOSITION OF FOREIGN GIFTS.**

Section 7342(f)(4) of Title 5, United States Code, is amended—

(1) by striking all that follows "(4)"; and

(2) inserting the following new paragraph:

"(4)(A) In transmitting such listings for an element of the Intelligence Community, as defined in section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4)), the head of an Intelligence Community element may delete the information described in subparagraphs (A) and (C) of paragraphs (2) and (3) if the head of that Intelligence Community element certifies in writing to the Secretary of State that the publication of such information could adversely affect United States intelligence sources or methods.

**SEC. 109. CANCELLATION OF CERTAIN REPORTING REQUIREMENTS**

CANCELLATION OF STATUTORY REPORTING REQUIREMENTS. – The requirements for the following reports are hereby cancelled:

(a) Unclassified Annual Report of the Intelligence Community as required by the National Security Act of 1947, as amended (50 U.S.C. 404d).

(b) Attorney General Annual Report on the Use of Appropriated Funds by the Office of Intelligence Policy and Review, section 606(b)(2)(A), Intelligence Authorization Act for FY2001, P.L. 106-567, 114 Stat. 2854.

(c) Annual Presidential Report Relating to Official Immunity in Interdiction of Aircraft Engaged in Illicit Drug Trafficking, section 503, Intelligence Authorization Act for FY2002, P.L. 107-108, 115 Stat. 1405.

(d) Annual Director of Central Intelligence Report on the Status of the Terrorist Identification Classification System, section 343(g), Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2400.

(e) Annual Reports by the Director of Central Intelligence [now DCIA], Director of NSA, Director of DIA, and Director of NIMA on Improvements of Financial Statements of Certain Elements of the Intelligence Community, section 823, Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2427.

(f) Annual Report by the Counterdrug Intelligence Coordinating Group on Current Counterdrug Intelligence Matters, section 826, Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2429.

(g) Annual Report by the Director, FBI on the exercise of FBI’s authority to enter into personal services contracts to support the intelligence or counterintelligence missions of the FBI, section 311, Intelligence Authorization Act for FY2004, P.L. 108-177, 117 Stat. 2605.

(h) Annual Report to Congress by the President on Actions Taken in Response to Espionage by the People's Republic of China (National Defense Authorization Act for Fiscal Year 2000, Section 3151 (42 U.S.C. § 7383e).

(i) Annual Review of Individuals Included on Dissemination Lists for Access to Classified Information (Intelligence Authorization Act for Fiscal Year 2004, Section 341(a) (50 U.S.C. § 442a).

(j) FY 1998 House Permanent Select Committee on Intelligence Unclassified Report, Intelligence Sharing with the United Nations, FY 1997 Intelligence Authorization Act, P.L. 104-293, Section 308(a) (50 U.S.C. 404g).

(k) Annual Report on Safety and Security of Russian Nuclear Facilities and Nuclear Military forces, National Security Act of 1947, as amended, section 114(b) (50 U.S.C. 404i(b).

(l) Annual Report Concerning Dismantling of Russian Strategic Nuclear Warheads - Moscow Treaty, FY 2004 Defense Authorization Conference Report, HR 108-354.

(m) Threat Reduction Interaction Between the Intelligence Community, the Department of Defense and the Department of Energy, FY 2001 Intelligence Authorization Classified Annex, pp. 11-12.

(n) Coastal State Territorial Claims and U.S. Reconnaissance Activity, FY 2005 Senate Select Committee on Intelligence Report 108-258, pp. 6-7.

(o) External Competitive Analysis on China-Taiwan, FY2000 House Permanent Select Committee on Intelligence Report, Classified Annex, pp. 93-94.

**Subtitle B. Efficient Management of Budget Authorities.**

**SEC. 110. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.**

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2008 the sum of $705,376,000. Within such amount, funds identified in the classified Schedule of Authorizations referred to in section 102(a) for advanced research and development shall remain available until September 30, 2009.

(b) CLASSIFIED AUTHORIZATIONS.— In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there is also authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2008 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a). Such additional amounts shall remain available until September 30, 2008, except for amounts authorized to be appropriated for research and development, which shall remain available until September 30, 2009.

**SEC. 111. AUTHORIZATION OF APPROPRIATIONS.**

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund for fiscal year 2008 the sum of $262,500,000.

**SEC. 112. MODIFICATION OF AVAILABILITY OF FUNDS FOR DIFFERENT INTELLIGENCE ACTIVITIES.**

Subparagraph (B) of section 504(a)(3) of the National Security Act of 1947 (50 U.S.C. 414(a)(3)) is amended to read as follows:

‘‘(B) the use of such funds for such activity supports an emergent need, improves program effectiveness, or increases efficiency; and’’.

**SEC. 113. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.**

The authorization of appropriations for salary, pay, retirement, and other benefits for Federal employees pursuant to this Act may be increased by such additional or supplemental amounts as may be necessary for increases in such compensation or benefits authorized by law.

**SEC. 114. RESERVE FOR CONTINGENCIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE.**

(a) ESTABLISHMENT. – Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.) as amended, is further amended by inserting after section 103G the following new section:

“RESERVE FOR CONTINGENCIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE

“(a) IN GENERAL. – There is hereby authorized a Reserve for Contingencies Fund of the OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE”.

“(b) ELEMENTS. -- The Reserve for Contingencies of the Director National Intelligence shall consist of the following elements:

“(1) Amounts authorized to be appropriated to the Reserve on an annual basis.

“(2) Amounts authorized to be transferred to or deposited in the Reserve by law.

“(c) AMOUNTS DEPOSITED. -- Amounts deposited into the Reserve for Contingencies of the Director of National Intelligence must be amounts appropriated to the National Intelligence Program, and may include an amount of appropriated funds subject to cancellation in accordance with 31 U.S.C. 1552.

“(d) LIMITATIONS ON AVAILABILITY OF FUNDS. – Amounts in the Reserve for Contingencies of the Director of National Intelligence –

“(1) shall be available for such purposes as are provided by law for the Office of the Director of National Intelligence or the separate elements of the intelligence community, including for a program or activity not previously authorized by Congress when the Director of National Intelligence has, consistent with the provisions of 50 U.S.C. sections 502 and 503, notified the congressional intelligence committees of the intention to utilize such amounts for such a purpose and 15 calendar days have elapsed from such notification and with the approval of the Director of the Office of Management and Budget; funds in the reserve can be used to support an emergent need, improvements to program effectiveness, or increased efficiency;”

“(2) shall be used subject to the direction and approval of the Director of National Intelligence or the Director’s designee and in accordance with procedures issued by the Director;

“(3) the annual appropriation shall not exceed $50,000,000 for any given fiscal year and the period of availability will be two years.”.

(b) CLERICAL AMENDMENT. – The table of contents in the first section of the National Security Act of 1947, as amended, is further amended by inserting after the item relating to section 103G the following new item:

“Sec. 103H. RESERVE FOR CONTINGENCIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE.”.

**SEC. 117. MULTIYEAR NATIONAL INTELLIGENCE PROGRAM.**

Section 1403 of the National Defense Authorization Act for Fiscal Year 1991, as amended, (50 U.S.C. 404b) is amended—

(1) in the headings for the section and for subsection (a), and in subsection (a), by striking “foreign”;

(2) in subsections (a) and (c), by striking “Director of Central Intelligence” and inserting “Director of National Intelligence”; and

(3) in subsection (b), by inserting “of National Intelligence” after “Director”.

**SEC. 118. REFERENCES TO MILITARY INTELLIGENCE PROGRAM AND RELATED ACTIVITIES.**

Section 102A of the National Security Act of 1947 (50 U.S.C. 403-1), as amended by section 1011(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended--

(1) in subsection (c)(3)(A),

(i) by striking the word “budgets” and inserting “budget”, and

(ii) by striking “Joint Military Intelligence Program and for Tactical Intelligence and Related Activities,” and inserting “Military Intelligence Program or for any successor program or programs”; and

(2) in subsection (d)(1)(B), by striking “Joint Military Intelligence Program,” and inserting “Military Intelligence Program or any successor program or programs.”.

**SEC. 120. CONFERENCES CONDUCTED BY ELEMENTS OF THE INTELLIGENCE COMMUNITY: COLLECTION OF FEES TO COVER COSTS.**

The National Security Act of 1947 is amended by adding the following new section at the end of Title I:

``ADDITIONAL INTELLIGENCE COMMUNITY AUTHORITIES

``Sec. 120. (a) Definitions-

(1) For purposes of this section, the terms 'agency' and 'element' refer to agencies and elements that are members of the Intelligence Community, as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a-4).

(2) For purposes of this section, the term ``conference'' includes, but is not limited to, events such as seminars, exhibitions, symposia, or similar meetings conducted by an agency or element.

(b) Authority to Collect Fees-

(1) An agency or element may collect fees from any individual or commercial participant in a conference.

(2) An agency or element may provide for the collection of fees under this section directly or through contract.

(3) Such fees may be collected in advance of a conference.

(c) Use of Collected Fees – Amounts collected under subsection (b) with respect to a conference –

(1) shall be credited to the appropriation or account from which the costs of the conference are paid; and

(2) shall be available to pay the costs and necessary expenses of the agency or element with respect to the conference; or

(3) shall be available to reimburse the agency or element for costs and necessary expenses incurred with respect to the conference.

(d) Treatment of Excess Amounts – In the event the total amount of fees collected under subsection (b) with respect to a conference exceeds the actual costs of the agency or element with respect to the conference, the amount of such excess shall be deposited into the Treasury as miscellaneous receipts.”

## Subtitle C. Modernizing Civilian Personnel Systems within the Intelligence Community.

### SEC. 121. ENHANCING PERSONNEL FLEXIBILITES THROUGHOUT THE INTELLIGENCE COMMUNITY.

The National Security Act of 1947 is amended by adding new paragraphs (t), (u) and (v) to section 102A as follows:

"(t) AUTHORITY TO ESTABLISH POSITIONS IN THE EXCEPTED SERVICE. (1) The Director of National Intelligence, with the concurrence of the head of the department or agency concerned, in coordination with the Director of the Office of Personnel Management, may—

"(A) convert such competitive service positions and their incumbents within elements of the Intelligence Community to excepted service positions as the Director determines necessary to carry out the intelligence functions of such elements of the Intelligence Community; and

"(B) establish the classification and ranges of rates of basic pay for such positions, notwithstanding otherwise applicable laws governing the classification and rates of basic pay for such positions.

“(2) At the request of the Director of National Intelligence, the heads of departments or agencies may establish new positions in the excepted service within the elements of their respective departments or agency that are part of the Intelligence Community, if the Director of National Intelligence determines such positions are necessary to carry out the intelligence functions of such elements of the Intelligence Community.

“(3) The Director of National Intelligence may establish the classification and ranges of rates of basic pay for any positions created under subsection (2), notwithstanding otherwise applicable laws governing the classification and rates of basic pay for such positions

“(4) The heads of the departments or agencies concerned are authorized to appoint individuals for service in such positions converted or created in subsections (1) and (2) without regard to the provisions of chapter 33 of title 5 governing appointments in the competitive service, and to fix the compensation of such individuals within the applicable ranges of rates of basic pay established by the Director of National Intelligence.

“(3) The maximum rate of basic pay allowed under authority of this subsection is the rate for level III of the Executive Schedule.

“(u) PAY AUTHORITY FOR CRITICAL POSITIONS.

“(1) Notwithstanding any pay limitation established under any other provision of law applicable to employees in elements of the Intelligence Community, the Director of National Intelligence, in consultation with the Directors of the Office of Personnel Management and the Office of Management and Budget, may grant authority to fix the rate of basic pay for 1 or more positions within the Intelligence Community at a rate in excess of any applicable limitation, subject to the conditions set forth in this subsection. Exercise of a granted authority is at the discretion of the head of the agency employing the individual in a position covered by the authority, subject to the conditions set forth in this subsection and any conditions established by the Director of National Intelligence when granting the authority

“(2) Authority under this subsection may be granted or exercised—

“(A) only with respect to a position which requires an extremely high level of expertise and is critical to successful accomplishment of an important mission; and

“(B) only to the extent necessary to recruit or retain an individual exceptionally well qualified for the position.

“(3) The rate of basic pay may not be fixed under this subsection at a rate greater than the rate payable for level II of the Executive Schedule, except upon written approval of the Director of National Intelligence or as otherwise authorized by law.

"(4) The rate of basic pay may not be fixed under this subsection at a rate greater than the rate payable for level I of the Executive Schedule, except upon written approval of the President in response to a request by the Director of National Intelligence or as otherwise authorized by law.

“(5) The authority granted under this subsection for a position shall terminate at the discretion of the Director of National Intelligence.”

“(v) EXTENDING PERSONNEL FLEXIBILITIES THROUGHOUT THE INTELLIGENCE COMMUNITY. (1) Notwithstanding the provisions of any other law and in order to ensure the equitable treatment of employees across the Intelligence Community, the Director of National Intelligence, with the concurrence of the head of the department or agency concerned, and for those matters that fall under the responsibilities of the Office

of Personnel Management under statute or Executive Order, in coordination with the Director of the Office of Personnel Management, may authorize an element or elements of the Intelligence Community, as defined in section 103 of this Act, to adopt compensation authority, performance management authority, and scholarship authority that have been authorized for any other element of the Intelligence Community, *provided that*—

"(A) the Director of National Intelligence determines that such adoption would improve the management and performance of the Intelligence Community, and

"(B) the Director of National Intelligence notifies the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence at least 60 days before any such particular authority is to take effect, and provides those committees with a description of the authority to be extended and an estimate of the costs associated therewith."

"(2) To the extent that an existing compensation authority within the Intelligence Community is limited to a particular category of employees or a particular situation, that authority may be adopted in another element of the Intelligence Community only for employees in an equivalent category or in an equivalent situation.

“(3) For the purpose of this subsection, the term ‘compensation authority’ means authority involving basic pay(including position classification), premium pay, awards, bonuses, incentives, allowances, differentials, student loan repayments, and special payments, excluding—

“(A) authorities related to benefits such as leave, severance pay, retirement, and insurance;

“(B) the authority to grant Presidential Rank Awards provided under 5 USC 4507 and 4507a, 5 USC 3151(c), or any other statute.

“(C) compensation authorities and performance management authorities provided under statutes pertaining to the Senior Executive Service.

**SEC. 125. CONTRIBUTIONS TO THRIFT SAVINGS PLAN.**

(a) Section 8351 of Title 5, United States Code, is amended-

(1) by adding a new subsection (f) to read as follows:

"(f)(1) Under regulations prescribed by the Executive Director in consultation with the Director of the Office of Personnel Management, an employee making contributions to the Thrift Savings Fund out of basic pay may also make an advance election to contribute by direct transfer to the Thrift Savings Fund all or any part of any payment, other than basic pay, as may be prescribed by regulation.

"(2) For purposes of subsection (b)(2)(C), an amount transferred to the Thrift Savings Fund under paragraph (a) shall constitute basic pay."; and

(2) in subsection (d) by-

(A) striking "(d)(1)" and inserting "(d)"; and

(B) repealing paragraph (2).

(b) Sections 8432(k) of Title 5, United States Code, is amended to read as follows-

"(k)(1) Under regulations prescribed by the Executive Director in consultation with the Director of the Office of Personnel Management, an employee making contributions to

the Thrift Savings Fund out of basic pay may also make an advance election to contribute by direct transfer to the Thrift Savings Fund all or any part of any payment, other than basic pay, as may be prescribed by regulation.

"(2) For purposes of subsection (c), basic pay of an employee shall not include an amount transferred to the Thrift Savings Fund under paragraph (1).

"(3) For purposes of subsection (a)(3), an amount transferred to the Thrift Savings Fund under paragraph (1) shall constitute basic pay."

(c) The amendments made by this section shall take effect at the time prescribed in regulations issued by the Executive Director.

**SEC. 126. REPEAL OF RESTRICTION ON THE USE OF NON-REIMBURSABLE DETAILEES.**

REIMBURSEMENT. – Except as provided in section 113 of the National Security Act of 1947 (50 U.S.C. 404h) and section 904(g)(2) of the Counterintelligence Enhancement Act of 2002 (title IX of Public Law 107-306)(50 U.S.C. 402c(g)(2)), and notwithstanding any other provision of law, during fiscal year 2008, or any fiscal year thereafter, any officer or employee of the United States or a member of the Armed Forces, who is detailed to the staff of an element of the Intelligence Community funded through the Community Management Account from another element of the United States Government, may be detailed on a reimbursable or non-reimbursable basis, as agreed to by the Director of National Intelligence and the head of the sending department or agency, or their respective designees for a period not to exceed three years.

## TITLE II – THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND INTELLIGENCE COMMUNITY MATTERS.

### SEC. 201. FEDERAL ADVISORY COMMITTEE ACT.

Section 4(b) of the Federal Advisory Committee Act (5 U.S.C. App. 2) is amended—

(1) in paragraph (1), by striking “or”;

(2) in paragraph (2), by striking the period and inserting “; or”; and

(3) by inserting at the end the following new paragraph:

``(3) the Office of the Director of National Intelligence.’’.

**SEC. 202. CLARIFICATION OF THE RESTRICTION AGAINST CO-LOCATION OF OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE HEADQUARTERS.**

Section 103(e) of the National Security Act of 1947, as amended (50 U.S.C. 403-3(e)), is further amended—

(1) by striking “Commencing” and inserting “(1) Commencing”;

(2) by striking “the Office” and inserting “the headquarters of the Office”;

(3) by striking “any other element” and inserting “the headquarters of any other element”;

(4) by inserting before the period at the end thereof “as defined in section 3(4) of the National Security Act of 1947, as amended”; and

(5) by adding the following new paragraph:

``(2) The President may waive the limitation in paragraph (1) of this subsection if the President determines

(A) that waiver would be in the interest of national security; or,

(B) that the additional cost of separate headquarters outweighs the potential benefits of the limitation.’’

**SEC. 203. APPLICATION OF THE PRIVACY ACT TO THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.**

Section 552a(j) of Title 5 is amended by:

(1) striking the word “or” at the end of subparagraph (j)(1);

(2) redesignating subparagraph (j)(2) as (j)(3),

(3) and by inserting after subparagraph (j)(1) the following new subparagraph (j)(2):

“(2) maintained by the Office of the Director of National Intelligence; or”.

**SEC. 205. PROTECTION OF CERTAIN FILES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.**

Title VII of the National Security Act of 1947 (50 U.S.C. 431 et seq.) is amended by adding at the end the following new section:

"PROTECTION OF CERTAIN FILES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

"Sec. 706. (a) RECORDS FROM EXEMPTED OPERATIONAL FILES.--(1) Records disseminated or otherwise provided to an element of the Office of the Director of National Intelligence from the exempted operational files of elements of the intelligence community designated in accordance with Title VII of this Act, and any operational files created by the Office of the Director of National Intelligence that incorporate such records in accordance with paragraph (A)(ii) below, shall be exempted from the provisions of section 552 of Title 5, United States Code that require search, review, publication or disclosure in connection therewith, in any instance where:

(A)(i) such record is shared within the Office of the Director of National Intelligence and not disseminated by that Office beyond that Office; or

(ii) such record is incorporated into new records created by personnel of the Office of the Director of

National Intelligence and maintained in operational files of the Office of the Director of National Intelligence and the records are not disseminated by that Office beyond that Office; and

(B) the operational files from which such records have been obtained continue to remain designated as operational files exempted from section 552 of Title 5, United States Code.

"(2) The operational files of the Office of the Director of National Intelligence referenced in paragraph (A)(ii) shall be similar in nature to the originating operational files from which the record was disseminated or provided, as such files are defined in Title VII of this Act."

"(3) Records disseminated or otherwise provided to the Office of the Director of National Intelligence from other elements of the intelligence community that are not protected by subsection (a)(1), and that are authorized to be disseminated beyond the Office of the Director of National Intelligence, will remain subject to search and review under section 552 of title 5, United States Code, but may continue to be exempted from the publication and disclosure provisions of that

section by the originating agency to the extent that the Act permits."

"(4) Notwithstanding the provisions of sections 701-705 of the National Security Act, records in the exempted operational files of the Central Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency or the Defense Intelligence Agency shall not be subject to the search and review provisions of section 552 of title 5 solely because they have been disseminated to an element or elements of the Office of the Director of National Intelligence, or referenced in operational files of the Office of the Director of National Intelligence and that are not disseminated beyond the Office of the Director of National Intelligence."

"(5)(A)Notwithstanding the provisions of sections 701-705 of the National Security Act, the incorporation of records from the operational files of the Central Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency or the Defense Intelligence Agency, into operational files of the Office of the Director of National

Intelligence shall not subject that record or the operational files of the Central Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency or the Defense Intelligence Agency to the search and review provisions of section 552 of title 5."

"(b) (1) Files in the Office of the Director of National Intelligence that are not exempted under subsection (a) of this section which contain information derived or disseminated from exempted operational files shall be subject to search and review."

"(2) The inclusion of information from exempted operational files in files of the Office of the Director of National Intelligence that are not exempted under subsection (a) of this section shall not affect the exemption of the originating operational files from search, review, publication, or disclosure."

"(3) Records from exempted operational files of the Office of the Director of National Intelligence which have been disseminated to and referenced in files that are not exempted under subsection (a) of this section and which have been returned to exempted

operational files of the Office of the Director of National Intelligence for sole retention shall be subject to search and review."

"(c) SUPERSEDURE OF OTHER LAWS. The provisions of this section may not be superseded except by a provision of law that is enacted after the date of the enactment of this section and that specifically cites and repeals or modifies such provisions.

"(d) APPLICABILITY. The Director of National Intelligence will publish a regulation listing the specific elements within the Office of the Director of National Intelligence whose records can be exempted under this provision.

"(e) ALLEGATION; IMPROPER WITHHOLDING OF RECORDS; JUDICIAL REVIEW.—(1) Except as provided in paragraph (2), whenever any person who has requested agency records under section 552 of Title 5, United States Code, alleges that the Office of the Director of National Intelligence has withheld records improperly because of failure to comply with any provision of this section, judicial review shall be available under the terms set forth in section 552(a)(4)(B) of Title 5, United States Code.

"(2) Judicial review shall not be available in the manner provided for under paragraph (1) as follows:

"(A) In any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign relations is filed with, or produced for, the court by the Office of the Director of National Intelligence, such information shall be examined ex parte, in camera by the court.

"(B) The court shall determine, to the fullest extent practicable, the issues of fact based on sworn written submissions of the parties.

"(C) When a complainant alleges that requested records are improperly withheld because of improper placement solely in exempted operational files, the complainant shall support such allegation with a sworn written submission based upon personal knowledge or otherwise admissible evidence.

"(D)(i) when a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, the Office of the Director of National Intelligence shall meet its burden under section 552(a)(4)(B) of Title 5, United States Code, by demonstrating to the court by sworn written submission that exempted operational files likely to contain responsive

records currently meet the criteria set forth in subsection (a) of this section.

"(ii) The court may not order the Office of the Director of National Intelligence to review the content of any exempted operational file or files in order to make the demonstration required under clause (i), unless the complainant disputes the Office's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence.

"(E) In proceedings under subparagraphs (C) and (D), the parties may not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admissions may be made pursuant to rules 26 and 36.

"(F) If the court finds under this subsection that the Office of the Director of National Intelligence has improperly withheld requested records because of failure to comply with any provision of this section, the court shall order the Office to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of Title 5, United States Code, and such order shall be the exclusive remedy for failure to comply with this section .

“(G) If at any time following the filing of a complaint pursuant to this paragraph the Office of the Director of National Intelligence agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.”

(f) CLERICAL AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting the following new item: “Sec. 706. Protection of Certain Files of the Office of the Director of National Intelligence.”.

**SEC. 206. STRENGTHENING ACCESS TO INFORMATION.**

Section 102A(g)(1) of the National Security Act of 1947, as amended (50 U.S.C. 403-1(g)(1)), is further amended--

(1) in subparagraph (E), by striking “and” after the semicolon;

(2) in subparagraph (F), by striking the period and inserting “; and”; and

(3) by adding at the end the following:

“(G) in the implementation of this subsection and without regard to any other provision of law other than this Act and Title I of the Intelligence Reform and Terrorism Prevention Act of 2004, expend funds for and direct the development and fielding of systems of common concern related to the collection, processing, analysis, exploitation, and dissemination of intelligence information, and any department or agency is authorized to receive and utilize such funds or systems; and

“(H) for the purpose of addressing critical gaps in intelligence information sharing capabilities, have the authority to transfer funds appropriated for a program within the National Intelligence Program to a program funded by appropriations not within the

National Intelligence Program, subject to the same terms and conditions as apply to a transfer of funds appropriated for a program within the National Intelligence Program to another such program under subsections (d)(3) through (d)(7) of this section, and under the National Security Intelligence Reform Act of 2004 (title I of the Intelligence Reform and Terrorism Prevention Act of 2004).”.

**SEC. 207. APPLICATION OF CERTAIN FINANCIAL REPORTING REQUIREMENTS TO DIRECTOR OF NATIONAL INTELLIGENCE.**

The Director of National Intelligence shall not be required to submit audited financial statements under section 3515 of title 31, United States Code for the Office of the Director of National Intelligence with respect to fiscal years 2008, and 2009.

**SEC. 208. PROTECTION OF INTELLIGENCE SOURCES AND METHODS FROM UNAUTHORIZED DISCLOSURE.**

Section 102A(i) of the National Security Act of 1947 (50 U.S.C. 403-1(i)) is further amended by striking paragraph (3).

**SEC. 209. PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT AND THE INFORMATION SHARING COUNCIL.**

(a) Subsection 1016(f)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) is amended by striking the phrase from the second sentence, ``during the two-year period beginning on the date of designation under this paragraph unless sooner'' and replacing it with "for the duration of the actions covered in the Information Sharing Environment Implementation Plan; however, the decision to continue the Program Manager shall be reviewed annually by the President until".

(b) The second sentence of Subsection 1016(g)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) is amended by – (1) striking the phrase ``two-year''.

(2) striking the phrase "unless sooner" and replacing it with "until".

**SEC. 214. MEMBERSHIP OF THE DIRECTOR OF NATIONAL INTELLIGENCE ON THE TRANSPORTATION SECURITY OVERSIGHT BOARD.**

Section 115(b)(1)(F) of title 49, United States Code, is amended by striking “The Director of the Central Intelligence Agency” and inserting “The Director of National Intelligence, or the Director’s designee.”.

**SEC. 215. TECHNICAL CORRECTIONS TO THE NATIONAL SECURITY ACT.**

Title I of the National Security Act of 1947, as amended by Title I of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended—

(1) in section 102A (50 U.S.C. 403-1)--

(i) in subsection (d)(3), by striking "subparagraph (A)" and inserting "paragraph (1)(A)";

(ii) in subsection (d)(5)(A), by striking "or personnel";

(iii) in subsection (l)(2)(B), by striking "section" and inserting "paragraph"; and

(2) in section 119(c)(2)(B) (50 U.S.C. 404o(c)(2)(B)), by striking "(h)" and inserting "(i)".

**SEC. 216. TECHNICAL CORRECTIONS TO INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.**

The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) is amended—

(1) in section 1011(n) (50 U.S.C. 403-1(n)), by striking “Acquisition Authorities” in the paragraph heading and inserting “Acquisition and Other Authorities”;

(2) in section 1016(e)(10)(B) (6 U.S.C. 485), by striking “Attorney General” the second time it appears and inserting “Department of Justice”;

(3) in section 1061(d)(4)(A) (5 U.S.C. 601 note), by striking “National Intelligence Director” and inserting “Director of National Intelligence”;

(4) in section 1071(e), by striking “(1)”;

(5) in the heading of section 1072(b), by inserting “Agency” after “Intelligence”;

(6) in section 2001 (28 U.S.C. 532 note)—

(i) in subsection (c)(1), by inserting “of” between “Investigation” and “an institutional culture”;

(ii) in subsection (e)(2), by striking “National Intelligence Director in a manner consistent with section 112(e)” and inserting “Director of National

Intelligence in a manner consistent with applicable law”;

(iii) in subsection (f), by striking the comma after “shall”; and

(7) in section 2006 (28 U.S.C. 509 note)—

(i) in subsection (2), by striking “the”;

(ii) in subsection (3), by striking “the specific” and inserting “specific”.

**SEC. 218. REPEAL OF CERTAIN AUTHORITIES RELATING TO THE OFFICE OF THE NATIONAL COUNTER-INTELLIGENCE EXECUTIVE.**

(a) REPEAL OF CERTAIN AUTHORITIES.—Section 904 of the Counterintelligence Enhancement Act of 2002 (title IX of Public Law 107–306; 50 U.S.C. 402c) is amended—

(1) by striking subsections (d), (g)(3), (g)(4), (h), (i), and (j); and

(2) by redesignating subsections (e), (f), (g), (k), (l), and (m) as subsections (d), (e), (f), (g), (h), and (i) respectively.

(b) CONFORMING AMENDMENTS.—That section is further amended—

(1) in subsection (d), as redesignated by subsection (a)(2) of this section, by striking ‘‘subsection (f)’’ each place it appears in paragraphs (1) and (2) and inserting ‘‘subsection (e)’’;

(2) in subsection (e)(1), as so redesignated, by striking ``subsection(e)(1)’’ and inserting “subsection (d)(1)’’; and

(3) in subsection (e)(2), as so redesignated, by striking ‘‘subsection (e)(2)’’ and inserting ‘‘subsection (d)(2)’’.

**SEC. 219. TECHNICAL CORRECTIONS TO EXECUTIVE SCHEDULE.**

(a) Section 5313 of title 5, United States Code, is amended by striking “Director of Central Intelligence” and inserting in lieu thereof “Director of the Central Intelligence Agency”.

(b) Section 5314 of title 5, United States Code, is amended by striking “Deputy Directors of Central Intelligence (2).”.

(c) Section 5315 of title 5, United States Code, is amended by striking “General Counsel to the National Intelligence Director” and inserting in lieu thereof “General Counsel of the Office of the Director of National Intelligence”.

## TITLE III – MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY.

### Subtitle A. Central Intelligence Agency

**SEC. 301. REPORT ON AUDITED FINANCIAL STATEMENTS PROGRESS.**

Section 114A of the National Security Act of 1947 (50 U.S.C. §404i-1), as amended by section 1071(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended by striking “the Director of the Central Intelligence Agency,”.

**SEC. 302. ADDITIONAL FUNCTIONS AND AUTHORITIES FOR PROTECTIVE PERSONNEL OF THE CENTRAL INTELLIGENCE AGENCY.**

Section 5(a)(4) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403f(a)(4)) is amended—

(1) by inserting ‘‘(A)’’ after ‘‘(4)’’;

(2) in subparagraph (A), as so designated—

(A) by striking ‘‘and the protection’’ and inserting ‘‘the protection’’; and

(B) by striking the semicolon and inserting ‘‘, and the protection of the Director of National Intelligence; and’’; and

(3) by adding at the end the following new subparagraph:

‘‘(B) Authorize personnel engaged in the performance of protective functions authorized pursuant to subparagraph (A), when engaged in the performance of such functions, to make arrests without warrant for any offense against the United States committed in the presence of such personnel, or for any felony cognizable under the laws of the United States, if such personnel have reasonable grounds to believe that the person to be arrested has committed or is committing such felony, except that any authority pursuant to this subparagraph may be exercised only in accordance with guidelines approved by the Director and the Attorney General. Such personnel may not exercise any authority for the service of civil process or the investigation of criminal offenses;’’.

**SEC. 303. DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.**

(a) ESTABLISHMENT AND DUTIES OF THE POSITION OF DEPUTY DIRECTOR OF CENTRAL INTELLIGENCE AGENCY.-- Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.), as amended by section 1011(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended by adding after section 104A the following:

"DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY"

"SEC. 104B. (a) DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.—There is a Deputy Director of the Central Intelligence Agency who shall be appointed by the President.

"(b) DUTIES OF DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.—(1) The Deputy Director of the Central Intelligence Agency shall assist the Director of the Central Intelligence Agency in carrying out the duties and responsibilities of the Director.

"(2) The Deputy Director of the Central Intelligence Agency shall act for, and exercise the powers of, the Director of the Central Intelligence Agency during the absence or disability of the Director of the Central Intelligence Agency, or during a vacancy in the

position of Director of the Central Intelligence Agency.”.

(b) EXECUTIVE SCHEDULE LEVEL III.—Section 5314 of title 5, United States Code, is amended by adding at the end the following new item:

“Deputy Director of the Central Intelligence Agency.”.

(c) EFFECTIVE DATE AND APPLICABILITY.—The amendments made by this section shall take effect on the date of the enactment of this Act and shall apply upon the earlier of--

(1) the date of the appointment by the President of an individual to serve as Deputy Director of the Central Intelligence Agency, except that the individual administratively performing the duties of the Deputy Director of the Central Intelligence Agency as of the date of the enactment of this Act may continue to perform such duties until the individual appointed to the position of Deputy Director of the Central Intelligence Agency assumes the duties of such position; or

(2) the date of the cessation of the performance of the duties of Deputy Director of the Central Intelligence Agency by the individual administratively performing such duties as of the date of the enactment of this Act.

**SEC. 304. TECHNICAL AMENDMENTS RELATING TO TITLES OF CENTRAL INTELLIGENCE AGENCY POSITIONS.**

Section 17(d)(3)(B)(ii) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q(d)(3)(B)(ii)) is amended—

(1) in subclause (I), by striking ''Executive Director'' and inserting ''Associate Deputy Director'';

(2) in subclause (II), by striking ''Deputy Director for Operations'' and inserting ''Director of the National Clandestine Service''; and

(3) in subclause (IV), by striking ''Deputy Director for Administration'' and inserting ''Director for Support''.

**SEC. 305. GENERAL COUNSEL OF THE CENTRAL INTELLIGENCE AGENCY.**

Section 20(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403t(a)) is amended by striking “, by and with the advice and consent of the Senate” and replacing it with a ".".

**SEC. 306. SECTION 5(a)(1) OF THE CENTRAL INTELLIGENCE AGENCY ACT OF 1949.**

Section 5(a)(1) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403f(a)(1)) is amended--

(1) by striking “any Agency functions or activities” and inserting “any functions or activities”; and

(2) by striking “authorized under paragraphs (2) and (3) of section 102(a), subsections (c)(7) and (d) of section 103, subsections (a) and (g) of section 104, and section 303 of the National Security Act of 1947 (50 U.S.C. 403(a)(2), (3), 403-3(c)(7), (d), 403-4(a), (g), and 405)” and inserting “authorized by law”.

**SEC. 308. TRAVEL ON ANY COMMON CARRIER FOR CERTAIN INTELLIGENCE COLLECTION PERSONNEL.**

Section 116(b) of the National Security Act of 1947 (50 U.S.C. 404k(b)), as amended by sections 1071(a)(1)(S), 1071(a)(3)(B), and 1072(a)(5) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), is further amended by inserting before the period the following: ``, who may redelegate such functions.''.

**SEC. 313. EXCLUSION OF GAIN FROM SALE OF A PRINCIPAL RESIDENCE BY CERTAIN EMPLOYEES OF THE INTELLIGENCE COMMUNITY.**

(a) SPECIAL RULE-Clause (vi) of subparagraph (C) of Section 121(d)(9) of the Internal Revenue Code of 1986 is amended by striking "such" and all that follows and inserting:

“(I) for purposes of such duty such employee has moved from one duty station to another, and

(II) at least one of such duty stations is located outside of the Washington, District of Columbia, and Baltimore metropolitan statistical areas (as defined by the Secretary of Commerce).”.

**SEC. 317. TECHNICAL MODIFICATION TO MANDATORY RETIREMENT PROVISION OF CENTRAL INTELLIGENCE AGENCY RETIREMENT ACT.**

Section 235(b)(1)(A) of the Central Intelligence Agency Retirement Act (50 U.S.C. 2055(b)(1)(A)) is amended to read as follows:

“(A) Upon reaching age 65, in the case of a participant in the system who is at the Senior Intelligence Service rank of level 4 or above;”.

## Subtitle B. Department of Defense

**SEC. 321. ENHANCEMENTS TO THE NATIONAL SECURITY AGENCY TRAINING PROGRAM.**

(a) TERMINATION OF EMPLOYEES.—Subsection (d)(1)(C) of section 16 of the National Security Agency Act of 1959 (50 U.S.C. 402 note) is amended by striking ‘‘terminated either by’’ and all that follows and inserting ‘‘terminated—

‘‘(i) by the Agency due to misconduct by the employee;

‘‘(ii) by the employee voluntarily; or

‘‘(iii) by the Agency for the failure of the employee to maintain such level of academic standing in the educational course of training as the Director of the National Security Agency shall have specified in the agreement of the employee under this subsection; and’’.

(b) AUTHORITY TO WITHHOLD DISCLOSURE OF AFFILIATION WITH NSA. – Subsection (e) of such section is amended by striking ‘‘(1) When an employee’’ and all that follows through ‘‘(2) Agency efforts’’ and inserting ‘‘Agency efforts’’.

**SEC. 322. ADDITIONAL FUNCTIONS AND AUTHORITIES FOR PROTECTIVE PERSONNEL OF THE NATIONAL SECURITY AGENCY.**

The National Security Agency Act of 1959 (50 U.S.C. section 402 note) is amended by adding at the end the following new section:

''SEC. 20. (a)

(1) Personnel of the Agency designated to perform protective functions pursuant to Department of Defense regulation are authorized, when engaged in the performance of such functions, to make arrests without a warrant for—

''(A) any offense against the United States committed in the presence of such personnel; or

''(B) any felony cognizable under the laws of the United States if such personnel have reasonable grounds to believe that the person to be arrested has committed or is committing such felony.

''(2) The authority in paragraph (1) may be exercised only in accordance with guidelines approved by the Director and the Attorney General.

''(3) Personnel of the Agency designated to perform protective functions pursuant to subsection (a) shall not exercise any authority for the service of civil process or the investigation of criminal offenses.

‘‘(b) Nothing in this section shall be construed to impair or otherwise affect any authority under any other provision of law relating to the performance of protective functions.’’.

**SEC. 323. TECHNICAL AMENDMENTS FOR THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY.**

(a) TECHNICAL CHANGES TO UNITED STATES CODE.- Titles 5 and 44 of the United States Code are amended by striking “National Imagery and Mapping Agency” each place it appears and inserting “National Geospatial-Intelligence Agency or any successor agency”.

(b) TECHNICAL CHANGES TO OTHER ACTS.- (1) Section 8H of the Inspector General Act of 1978 (Pub. L. 95-452; 5 USC App.) is amended by striking “National Imagery and Mapping Agency” and inserting “National Geospatial-Intelligence Agency or any successor agency”.

(2) Section 7(b)(2)(A)(i) of the Employee Polygraph Protection Act of 1988 (Pub. L. 100-347; 29 USC section 2006(b)(2)(A)(i)) is amended by striking “National Imagery and Mapping Agency” and inserting “National Geospatial-Intelligence Agency or any successor agency”.

(3) Section 207(a)(2)(B) of the Legislative Branch Appropriations Act, 1993 (Pub. L. 102-392; 44 USC section 501 note), is amended by striking “National Imagery and Mapping Agency” and inserting “National Geospatial-Intelligence Agency or any successor agency”.

(4) Section 201 of the Homeland Security Act of 2002 (Pub. L. 107-296; 6 USC section 121) is amended by striking “National Imagery and Mapping Agency” and inserting “National Geospatial-Intelligence Agency or any successor agency”.

## Subtitle C. Department of State; Department of Treasury; Federal Bureau of Investigation; Department of Homeland Security.

**SEC. 354. ELIMINATION OF REPORTING REQUIREMENT FOR THE DEPARTMENT OF THE TREASURY.**

Section 342 of the Intelligence Authorization Act for Fiscal Year 2003 (Pub. L. 107-306; 50 U.S.C. section 404m) is amended-

(1) by striking ``SEMIANNUAL REPORT ON'' from the title, and inserting ``EMERGENCY NOTIFICATION REGARDING'';

(2) by striking paragraphs (a) and (c); and

(3) renumbering paragraphs (b) and (d) as (a) and (b) respectively.

**SEC. 355. CLARIFYING AMENDMENTS RELATING TO SECTION 105 OF THE INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2004.**

(a) Section 105(b) of the Intelligence Authorization Act for Fiscal Year 2004 (Public Law 108–177; 117 Stat. 2603; 31 U.S.C. 311 note) is amended—

(1) by striking ‘‘Director of Central Intelligence’’ and inserting ‘‘Director of National Intelligence’’; and

(2) by inserting ‘‘or in section 313 of such 10 title,’’ after ‘‘subsection (a)),’’.

(b) Section 105(c) of the Intelligence Authorization Act for Fiscal Year 2004 (Public Law 108–177; 117 Stat. 2603; 31 U.S.C. 311 note) is amended by striking ‘‘DCI’’ and inserting ‘‘DNI’’.

**SEC. 360. DEPARTMENT OF HOMELAND SECURITY INFORMATION.**

(a) Section 1405 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Pub. L. 109-364) (10 U.S.C. section 130d) is amended as follows:

(1) in the section heading—

(A) by striking “certain”;

(B) by inserting “business information and homeland security” after “confidential”;

(2) in subsection (a), by striking “§ 130d.” and all that follows and inserting the following:

“§ 130d. Treatment under the Freedom of Information Act of confidential business information and homeland security information shared with State and local personnel.

“The sharing of confidential business information or homeland security information, pursuant to section 892 of the Homeland Security Act of 2002 (6 U.S.C. 482), by any Federal agency, with State and local personnel (as defined in such section) shall not be considered release of such information to the public, and shall not constitute a waiver of any applicable exemption to the release of such information under section 552 of title 5.”

(3) in subsection (b), by striking “130d.” and all that follows and inserting the following:

“130d. Treatment under the Freedom of Information Act of confidential business information and homeland security information shared with State and local personnel.”.

**SEC. 361. TECHNICAL AMENDMENT RELATING TO THE COAST GUARD INTELLIGENCE ELEMENT.**

Section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a) is amended as follows—

(a) in subparagraph (H), by inserting “the Coast Guard,” after “the Marine Corps,”; and

(b) in subparagraph (K), by striking “, including the Office of Intelligence of the Coast Guard”.

## TITLE IV – MATTERS RELATING TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

### SEC. 400. SHORT TITLE

Sections 400 through 414 may be cited as the ‘‘Foreign Intelligence Surveillance Modernization Act of 2007’’.

**SEC. 401. DEFINITIONS.**

(a) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is amended—

(1) in subparagraph (B), by striking ‘‘; or’’ and inserting ‘‘;’’; and

(2) by adding at the end the following:

‘‘(D) is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the certification required under section 104(a)(6) or 303(a)(6) contains a description of the kind of significant foreign intelligence information sought;’’.

(b) ELECTRONIC SURVEILLANCE.—Subsection (f) of such section is amended to read as follows:

‘‘(f) ‘Electronic surveillance’ means—

‘‘(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable

expectation of privacy and a warrant would be required for law enforcement purposes; or

‘‘(2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.’’.

(c) WIRE COMMUNICATION. —Subsection (l) of such section is amended by striking subsection (l).

(d) MINIMIZATION PROCEDURES.—Subsection (h) of such section is amended—

(1) in subsection (3) by striking “; and” and inserting “.”; and

(2) by striking subsection (4).

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

‘‘(n) ‘Contents’, when used with respect to a communication, includes any information concerning the substance, purport, or meaning of that communication.’’

**SEC. 402. ATTORNEY GENERAL AUTHORIZATION FOR ELECTRONIC SURVEILLANCE.**

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended by striking section 102 and inserting the following:

''AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

''SEC. 102. (a) IN GENERAL.— Notwithstanding any other law, the President, acting through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General—

''(1) certifies in writing under oath that—

''(A) the electronic surveillance is directed at—

''(i) the acquisition of the contents of communications of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a); or

''(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the control

of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a); and

‘‘(B) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

‘‘(2) reports such minimization procedures and any changes thereto to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate at least 30 days prior to the effective date of such minimization procedures, unless the Attorney General determines immediate action is required and promptly notifies the committees of such minimization procedures and the reason for their becoming effective immediately.

‘‘(b) MINIMIZATION PROCEDURES.—An electronic surveillance authorized under this section may be conducted only in accordance with the Attorney General’s certification and the minimization procedures. 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 the provisions of section 108(a).

''(c) SUBMISSION OF CERTIFICATION.—The Attorney General shall promptly transmit under seal to the court established under section 103(a) a copy of the certification under subsection (a)(1). Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—

''(1) an application for a court order with respect to the surveillance is made under section 104; or

''(2) the certification is necessary to determine the legality of the surveillance under section 106(f).

''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 electronic surveillance under section 102 or 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 electronic surveillance or 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 electronic surveillance or 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 24 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.''.

''USE OF INFORMATION ACQUIRED UNDER SECTION 102A

''SEC. 102C. (a) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to section 102A concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by section 102A. No otherwise privileged communication obtained in accordance with,

or in violation of, the provisions of section 102A shall lose its privileged character. No information from an acquisition pursuant to section 102A may be used or disclosed by Federal officers or employees except for lawful purposes.

‘‘(b) NOTIFICATION BY UNITED STATES.—Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against a person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, any information obtained or derived from such acquisition, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or so use that information or submit it in evidence, notify such person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

‘‘(c) NOTIFICATION BY STATES OR POLITICAL SUBDIVISION.—Whenever any State or political

subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against a person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, any information obtained or derived from such acquisition, the State or political subdivision thereof shall notify such person, the court, or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

''(d) MOTION TO SUPPRESS.—(1) Any person against whom evidence obtained or derived from an acquisition authorized pursuant to section 102A is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress

the evidence obtained or derived from such acquisition on the grounds that—

''(A) the information was unlawfully acquired; or

''(B) the acquisition was not properly made in conformity with an authorization under section 102A.

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

''(e) IN CAMERA AND EX PARTE REVIEW BY DISTRICT COURT.—Whenever a court or other authority is notified pursuant to subsection (b) or (c) of this section, or whenever a motion is made pursuant to subsection (d) of this section, or whenever any motion or request is made pursuant to any other statute or rule of the United States or any State by a person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A before any court or other authority of the United States or any State—

‘‘(1) to discover or obtain applications or orders or other materials relating to an acquisition authorized pursuant to section 102A, or

‘‘(2) to discover, obtain, or suppress evidence or information obtained or derived from an acquisition authorized pursuant to section 102A, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the acquisition as may be necessary to determine whether such acquisition was lawfully authorized and conducted. In making this determination, the court may disclose to the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, under appropriate

security procedures and protective orders, portions of the application, order, or other materials relating to the acquisition only where such disclosure is necessary to make an accurate determination of the legality of the acquisition.

''(f) SUPPRESSION OF EVIDENCE; DENIAL OF MOTION.—If the United States district court, pursuant to subsection (e) of this section, determines that an acquisition authorized pursuant to section 102A was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the acquisition or otherwise grant the motion of the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A. If the court determines that such acquisition was lawfully authorized and conducted, it shall deny the motion of the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A except to the extent that due process requires discovery or disclosure.

‘‘(g) FINALITY OF ORDERS.—Orders granting motions or requests under subsection (f) of this section, decisions under this section that an acquisition was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to an acquisition shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

‘‘(h) CONSULTATION WITH LAW ENFORCEMENT OFFICERS.—(1). Federal officers who acquire foreign intelligence information pursuant to section 102A may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against—

‘‘(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

''(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

''(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

''(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 102A.

"(i) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.".

(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.

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

**SEC. 403. JURISDICTION OF FISA COURT.**

Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—

(1) in subsection (a), by inserting ‘‘at least’’ before ‘‘seven of the United States judicial circuits’’; and

(2) by adding at the end the following new subsection:

‘‘(g) Applications for a court order under section 104 of this title are authorized if the Attorney General approves such applications to the court having jurisdiction under this section, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.’’.

**SEC. 404. APPLICATIONS FOR COURT ORDERS.**

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

(1) in subsection (a)—

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

(B) by redesignating paragraphs (3) through (10) as paragraphs (2) through (9), respectively;

(C) in paragraph (5), as redesignated by subparagraph (B), by striking ‘‘detailed description’’ and inserting ‘‘summary description’’;

(D) in paragraph (6), as redesignated by subparagraph (B)—

(i) in the matter preceding subparagraph (A), by striking ‘‘or officials designated’’ and all that follows through ‘‘consent of the Senate’’ and inserting ‘‘designated by the President to authorize electronic surveillance for foreign intelligence purposes’’;

(ii) in subparagraph (C), by striking ‘‘techniques;’’ and inserting ‘‘techniques; and’’;

(iii) by striking subparagraph (D); and

(iv) by redesignating subparagraph (E) as subparagraph (D);

(E) in paragraph (7), as redesignated by subparagraph (B), by striking ‘‘a statement of the means’’ and inserting ‘‘a summary statement of the means’’;

(F) in paragraph (8), as redesignated by subparagraph (B)—

(i) by striking ‘‘a statement’’ and inserting ‘‘a summary statement’’; and

(ii) by striking ‘‘application;’’ and inserting ‘‘application; and’’; and

(G) in paragraph (9), as redesignated by subparagraph (B), by striking "; and" and inserting "."

(2) by striking subsection (b);

(3) by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and

(4) in paragraph (1)(A) of subsection (d), as redesignated by paragraph (3), by striking ‘‘or the Director of National Intelligence’’ and inserting ‘‘the Director of National Intelligence, or the Director of the Central Intelligence Agency’’.

**SEC. 405. ISSUANCE OF AN ORDER.**

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

(1) in subsection (a)—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively;

(2) in paragraph (1) of subsection (c)—

(A) in subparagraph (D), by striking ‘‘surveillance;’’ and inserting ‘‘surveillance; and’’;

(B) in subparagraph (E), by striking ‘‘approved; and’’ and inserting ‘‘approved.’’; and

(C) by striking subparagraph (F).

(3) by striking subsection (d);

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

(5) in subsection (d), as redesignated by paragraph (4)—

(A) by striking “120 days” and insert “one year”, and

(B) by amending paragraph (2) to read as follows: ‘‘(2) Extensions of an order issued under this title may be granted on the same basis as an original order

upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not to exceed one year.’’;

(6) in subsection (e), as redesignated by paragraph (4), to read as follows:

‘‘(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—

‘‘(1) determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

‘‘(2) determines that the factual basis for issuance of an order under this title to approve such electronic surveillance exists;

‘‘(3) informs a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

‘‘(4) makes an application in accordance with this title to a judge having jurisdiction under section 103

as soon as practicable, but not more than 168 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, which ever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United

States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information is significant foreign intelligence information or indicates a threat of death or serious bodily harm to any person. The Attorney General shall assess compliance with the requirements of the prior sentence and shall include such assessments in the Attorney General's reports under section 102(b). A denial of the application made under this subsection may be reviewed as provided in section 103.'';

(7) in subsection (h), as redesignated by paragraph (4)—

(A) by striking ''a wire or'' and inserting ''an''; and

(B) by striking ''physical search'' and inserting ''physical search or in response to a certification by the Attorney General or a designee of the Attorney General seeking information, facilities, or technical assistance from such person under section 102B''; and

(8) by adding at the end the following new subsection:

‘‘(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842(d)(2) of this title; such information shall not be subject to minimization procedures.’’.

**SEC. 406. USE OF INFORMATION.**

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

(1) in subsection (i)—

(A) by striking ‘‘radio communication’’ and inserting ‘‘communication’’; and

(B) by striking ‘‘contents indicates’’ and inserting ‘‘contents contain significant foreign intelligence information or indicate’’; and

(2) by inserting after subsection (k) the following”

“(l) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.”.

**SEC. 407. WEAPONS OF MASS DESTRUCTION.**

(a) DEFINITIONS.—

(1) Subsection (a)(4) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)(4)) is amended by inserting ‘‘or the international proliferation of weapons of mass destruction’’ after ‘‘international terrorism’’.

(2) Subsection (b)(1) of such section (50 U.S.C. 1801(b)(1)) is amended—

(A) in subparagraph (C), by striking ‘‘; or’’ and inserting ‘‘;’’; and

(B) by adding at the end the following new subparagraphs:

‘‘(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

‘‘(F) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or’’.

(3) Subsection (e)(1)(B) of such section (50 U.S.C. 1801(e)(1)(B)) is amended by striking ‘‘sabotage or international terrorism’’ and inserting ‘‘sabotage,

international terrorism, or the international proliferation of weapons of mass destruction’’.

(4) Subsection (l) of such section (50 U.S.C. 1801(l)) is amended to read as follows:

‘‘(l) ‘Weapon of mass destruction’ means—

‘‘(1) any destructive device (as such term is defined in section 921 of title 18, United States Code) that is intended or has the capability to cause death or serious bodily injury to a significant number of people;

‘‘(2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

‘‘(3) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of title 18, United States Code); or

‘‘(4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.’’.

(b) USE OF INFORMATION.—

(1) Section 106(k)(1)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(k)(1)(B)) is amended by striking ‘‘sabotage or international

terrorism’’ and inserting ‘‘sabotage, international terrorism, or the international proliferation of weapons of mass destruction’’.

(2) Section 305(k)(1)(B) of such Act (50 U.S.C. 1825(k)(1)(B)) is amended by striking ‘‘sabotage or international terrorism’’ and inserting ‘‘sabotage, international terrorism, or the international proliferation of weapons of mass destruction’’.

**SEC. 408. LIABILITY DEFENSE.**

(a) IN GENERAL.—Notwithstanding any other law, and in addition to the immunities, privileges, and defenses provided by any other source of law, no action shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or any other form of assistance, during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act, in connection with any alleged classified communications intelligence activity that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, would be, or would have been intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.

(b) JURISDICTION.—Any action or claim described in subsection (a) that is brought in a State court shall be deemed to arise under the Constitution and laws of the

United States and shall be removable pursuant to section 1441 of title 28, United States Code.

(c) DEFINITIONS.—In this section:

(1) INTELLIGENCE COMMUNITY.—The term ‘‘intelligence community’’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(2) PERSON.—The term ‘‘person’’ has the meaning given the term in section 2510(6) of title 18, United States Code.

**SEC. 409. AMENDMENTS FOR PHYSICAL SEARCHES.**

(a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—

(1) in subsection (a)—

(A) by striking paragraph (2);

(B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively;

(C) in paragraph (2), as redesignated by subparagraph (B), by striking ‘‘detailed description’’ and inserting ‘‘summary description’’;

(D) in paragraph (3)(C), as redesignated by subparagraph (B), by inserting “or is about to be” before “owned”;

(E) in paragraph (6), as redesignated by subparagraph (B)—

(i) in the matter preceding subparagraph (A), by striking ‘‘or officials’’ and all that follows through ‘‘consent of the Senate’’ and inserting ‘‘designated by the President to authorize physical searches for foreign intelligence purposes’’;

(ii) in subparagraph (C), by striking ‘‘techniques;’’ and inserting ‘‘techniques; and’’;

(iii) by striking subparagraph (D);

(iv) by redesignating subparagraph (E) as subparagraph (D); and

(v) in subparagraph (D), as redesignated by clause (iv), by striking ‘‘certifications required by subparagraphs (C) and (D)’’ and inserting ‘‘certification required by subparagraph (C)’’; and

(F) in paragraph (8), as redesignated by subparagraph (B), by striking ‘‘a statement’’ and inserting ‘‘a summary statement’’; and

(2) in subsection (d)(1)(A), by striking ‘‘or the Director of National Intelligence’’ and inserting ‘‘the Director of National Intelligence, or the Director of the Central Intelligence Agency’’.

(b) ORDERS.—Section 304 of such Act (50 U.S.C. 1824) is amended—

(1) in subsection (a)—

(A) by striking paragraph (1);

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and

(C) in paragraph (2)(B), as redesignated by subparagraph (B), by inserting “or is about to be” before “owned”;

(2) in subsection (e), to read as follows:

‘‘(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—

‘‘(1) determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;

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

‘‘(3) informs a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ an emergency physical search; and

‘‘(4) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not more

than 168 hours after the Attorney General authorizes such physical search. If the Attorney General authorizes such emergency employment of a physical search, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or

political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information is significant foreign intelligence information or indicates a threat of death or serious bodily harm to any person. The Attorney General shall assess compliance with the requirements of the prior sentence and shall include such assessments in the Attorney General's reports under section 302(a)(2). A denial of the application made under this subsection may be reviewed as provided in section 103.''.

(c) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—

(1) in section 304(a)(5), by striking ''303(a)(7)(E)'' and inserting ''303(a)(6)(E)''; and

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

**SEC. 410. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.**

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

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

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

**SEC. 411. MANDATORY TRANSFER FOR REVIEW.**

(a) IN GENERAL.—In any case before any court challenging the legality of a classified communications intelligence activity relating to a foreign threat, or in which the legality of any such activity is in issue, if the Attorney General files an affidavit under oath that the case should be transferred to the Foreign Intelligence Surveillance Court because further proceedings in the originating court would harm the national security of the United States, the originating court shall transfer the case to the Foreign Intelligence Surveillance Court for further proceedings under this section.

(b) PROCEDURES FOR REVIEW.—The Foreign Intelligence Surveillance Court shall have jurisdiction as appropriate to determine standing and the legality of the communications intelligence activity to the extent necessary for resolution of the underlying case. All proceedings under this paragraph shall be conducted in accordance with the procedures set forth in section 106(f) of the Foreign Intelligence Surveillance Act of 1978, except that the Foreign Intelligence Surveillance Court shall not require the disclosure of national security information to any person without the approval of the

Director of National Intelligence or the Attorney General, unless in the context of a criminal proceeding, disclosure would be constitutionally required. Any such constitutionally required disclosure shall be governed by the Classified Information Procedures Act, Pub. L. No. 96-456, 94 Stat. 2025 (1980), or if applicable, Title 18, United States Code, Section 2339B(f).

(c) APPEAL, CERTIORARI, AND EFFECTS OF DECISIONS.—The decision of the Foreign Intelligence Surveillance Court made under paragraph (b), including a decision that the disclosure of national security information is constitutionally required, shall be subject to review by the Court of Review established under section 103(b) of the Foreign Intelligence Surveillance Act. The Supreme Court of the United States shall have jurisdiction to review decisions of the Court of Review by writ of certiorari granted upon the petition of the United States. The decision by the Foreign Intelligence Surveillance Court shall otherwise be binding in all other courts.

(d) DISMISSAL.—The Foreign Intelligence Surveillance Court or a court that is an originating court under paragraph (a) may dismiss a challenge to the legality of a classified communications intelligence activity for any reason provided for under law.

(e) PRESERVATION OF LITIGATION PRIVILEGES.—All litigation privileges shall be preserved in the originating court and in the Foreign Intelligence Surveillance Court, the Foreign Intelligence Court of Review, and the Supreme Court of the United States, in any case that is transferred and received under this section.

**SEC. 412. TECHNICAL AND CONFORMING AMENDMENTS.**

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

(1) in section 103(e)—

(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)’’;

(2) in section 105—

(A) in subsection (a)(4), as redesignated by section 105(1)(B)—

(i) by striking ‘‘104(a)(7)(E)’’ and inserting ‘‘104(a)(6)(D)’’; and

(ii) by striking ‘‘104(d)’’ and inserting ‘‘104(c)’’;

(B) in subsection (c)(1)(A), by striking ‘‘104(a)(3)’’ and inserting ‘‘104(a)(2)’’;

(3) in section 106—

(A) in subsection (j), in the matter preceding paragraph (1), by striking ‘‘105(e)’’ and inserting ‘‘105(d)’’; and

(B) in subsection (k)(2), by striking ‘‘104(a)(7)(B)’’ and inserting ‘‘104(a)(6)(B)’’; and

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

**SEC. 413. EFFECTIVE DATE.**

(a) Except as otherwise provided, the amendments made by this Act shall take effect 90 days 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. 414. CONSTRUCTION; SEVERABILITY.**

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

## SECTIONAL ANALYSIS

## TITLE I - INTELLIGENCE ACTIVITIES.

### Subtitle A. General Provisions.

*Sec. 101. Authorization of Appropriations.*

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for fiscal year 2008.

*Sec. 102. Classified Schedule of Authorizations.*

Section 102 makes clear that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities covered under this title for fiscal year 2008 are contained in a classified Schedule of Authorizations. The Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

*Sec. 103. Elimination of Certain Personnel Management Constraints.*

This section would add a new subsection to the National Security Act of 1947 to eliminate congressionally imposed civilian end-strength ceilings on the Intelligence Community. This section is consistent with the Strategic Plan of the Director of National Intelligence. Such ceilings, contained in recent Intelligence Authorization Acts, are inflexible, lead to increased use of contractors to perform necessary IC functions in lieu of staff employees, and severely hinder the IC's civilian joint duty, student employment, and National Intelligence Reserve Corps programs.

This proposal would repeal personnel ceilings and make future IC employment totals determined strictly by the overall budget appropriation. Congressional oversight of the IC workforce is assured by a requirement for an annual projection of employment levels based on mission requirements from the DNI to the intelligence oversight committees in each year's budget submission. This proposal is similar to legislation enacted by Congress for the Department of Defense, and codified at 10 U.S.C. 129.

This proposal will eliminate the need for the personnel ceilings adjustments authority that was included in section 103 of the previous Intelligence Authorization Acts.

*Sec. 104. Restriction on Conduct of Intelligence Activities.*

Section 104 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

*Sec. 105. Definition of Intelligence Community.*

Section 105 further amends section 3(4)(L) of the National Security Act of 1947, as amended by section 1073 of the Intelligence Reform and Terrorism Prevention Act of 2004, to strike the anomalous occurrence of the term “other” from the definition of “intelligence community”.

*Sec. 106. Additional Administrative Authorities for the Office of the Director of National Intelligence.*

Section 106 recognizes that from an organizational standpoint, the Director of National Intelligence (DNI) must be able to focus the Intelligence Community (IC) rapidly on a particular intelligence issue through a coordinated effort that uses all available resources. The DNI should have the ability to respond with flexibility and coordinate the IC response to an emerging threat or issue. Often times, the appropriate response is a small, limited duration inter-agency board or commission to examine the threat or issue and report back to the DNI. Other times, it may be the rapid establishment of a national intelligence center. Given the federated nature of the intelligence community, which crosses many organization lines, the application of the general prohibition against funding inter-agency boards and commissions to the intelligence community should be modified to permit limited exceptions.

To provide the necessary operational and organizational flexibility, this section grants the DNI the authority – notwithstanding certain specified provisions of general appropriations law – to approve interagency financing of national intelligence centers (authorized under Section 119B) of the National Security Act of 1947 (50 U.S.C. section 404o-2)) and of other boards, commissions, councils, committees, or similar groups established by the DNI (e.g., “mission managers,” as recommended by the Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction (WMD Commission)). Under this section, the DNI could authorize the pooling of resources from various IC agencies to finance national intelligence centers or other organizational groups designed to address identified intelligence matters. Upon the request of the DNI, the provision expressly permits intelligence community elements to fund or participate in the funding of, the authorized activities.

Section 106 also exempts the DNI from the provisions of the Administrative Procedures Act in the performance of his duties; this authority is similar to what the Director of Central Intelligence had.

*Sec. 108. Extension to the Intelligence Community of Authority to Delete Information about Receipt and Disposition of Foreign Gifts.*

Section 108 provides to the heads of Intelligence Community (IC) elements the same exemption from certain reporting requirements under 5 U.S.C. 7342 as the Central Intelligence Agency (CIA) and the Office of the Director of National Intelligence (ODNI) have. This section only applies to certain reporting requirements. Receipt of gifts must still comply with all applicable ethics laws and regulations.

Current law generally requires that detailed information about the receipt of foreign gifts be reported, including the source of the gift. In addition, some of this information subsequently is published in the Federal Register. Revealing the source of a gift given in the context of a foreign intelligence relationship would compromise the relationship and undermine national security.

To resolve this dilemma, the law provided an exemption to the former Director of Central Intelligence (DCI) from reporting information about foreign gifts, when the publication of the information could adversely affect United States intelligence sources. A similar exemption was extended to the Director of National Intelligence (DNI) and the Director of the Central Intelligence Agency (D/CIA) in section 1079 of the Intelligence Reform and Terrorism Prevent Act of 2004, Pub. L. No. 108-458 (Dec. 17, 2004).

Section 108 amends existing law to provide to the heads of the each IC element the same limited exemption from specified public reporting requirements that is currently authorized for the DNI and the D/CIA. The national security concerns that prompted the initial DCI exemption, and the more recent exemptions for the DNI and the D/CIA, apply with equal weight to other IC elements: the publication of certain information relating to foreign gifts or decorations provided to employees of IC agencies could adversely affect United States intelligence sources.

Section 108 supports two Enterprise Objectives identified in the National Intelligence Strategy: EO6, “Establish new and strengthen existing foreign intelligence relationships to help us meet global security challenges,” and E07,

“Create clear, uniform security practices and rules that allow us to work together, protect our nation’s secrets, and enable aggressive counterintelligence activities.” In particular, section 108 promotes the EO6 goal of strengthening existing foreign intelligence relationships and paving the way to ensure that new foreign alliances and partnerships will not be endangered by the threat that the classified relationship will be made public. Section 108 also promotes the EO7 goal of personnel security by protecting the names of certain Intelligence Community employees as well as ensuring the protection of classified information.

*Sec. 109. Cancellation of Certain Reporting Requirements.*

Section 109 cancels outdated and duplicative statutory reporting requirements. As part of an overall effort to reduce the number of outdated and duplicative reports to the Congress, the Intelligence Community also will seek agreement from the interested congressional committees to cancel other reporting requirements that originated in committee and conference reports and annexes to bills considered in one or both houses.

Section 109 cancels the requirements for the following statutory reports:

1. Unclassified Annual Report of the Intelligence Community as required by the National Security Act of 1947, as amended (50 U.S.C. 404d).

2. Attorney General Annual Report on the Use of Appropriated Funds by the Office of Intelligence Policy and Review, section 606(b)(2)(A), Intelligence Authorization Act for FY2001, P.L. 106-567, 114 Stat. 2854.

3. Annual Presidential Report Relating to Official Immunity in Interdiction of Aircraft Engaged in Illicit Drug Trafficking, section 503, Intelligence Authorization Act for FY2002, P.L. 107-108, 115 Stat. 1405.

4. Annual Director of Central Intelligence [now DNI] Report on the Status of the Terrorist Identification Classification System, section 343(g), Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2400.

5. Annual Reports by the Director of Central Intelligence [now DCIA], Director of NSA, Director of DIA, and Director of NIMA [now NGA] on Improvements of Financial Statements of Certain Elements of the Intelligence Community, section 823, Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2427.

6. Annual Report by the Counterdrug Intelligence Coordinating Group on Current Counterdrug Intelligence Matters, section 826, Intelligence Authorization Act for FY2003, P.L. 107-306, 116 Stat. 2429.

7. Annual Report by the Director, FBI on the exercise of FBI’s authority to enter into personal services contracts

to support the intelligence or counterintelligence missions of the FBI, section 311, Intelligence Authorization Act for FY2004, P.L. 108-177, 117 Stat. 2605.

8. Annual Report to Congress by the President on Actions Taken in Response to Espionage by the People's Republic of China (National Defense Authorization Act for Fiscal Year 2000, Section 3151 (42 U.S.C. 7383e).

9. Annual Review of Individuals Included on Dissemination Lists for Access to Classified Information (Intelligence Authorization Act for Fiscal Year 2004, Section 341(a) (50 U.S.C. § 442a).

10. FY 1998 House Permanent Select Committee on Intelligence Unclassified Report, Intelligence Sharing with the United Nations, FY 1997 Intelligence Authorization Act, P.L. 104-293, Section 308(a) (50 U.S.C. 404g).

11. Annual Report on Safety and Security of Russian Nuclear Facilities and Nuclear Military forces, National Security Act of 1947, as amended, section 114(b) (50 U.S.C. 404i(b).

12. Annual Report Concerning Dismantling of Russian Strategic Nuclear Warheads - Moscow Treaty, FY 2004 Defense Authorization Conference Report, HR 108-354.

13. Threat Reduction Interaction Between the Intelligence Community, the Department of Defense and the Department of Energy, FY 2001 Intelligence Authorization Classified Annex, pp. 11-12.

14. Coastal State Territorial Claims and U.S. Reconnaissance Activity, FY 2005 Senate Select Committee on Intelligence Report 108-258, pp. 6-7.

15. External Competitive Analysis on China-Taiwan, FY2000 House Permanent Select Committee on Intelligence Report, Classified Annex, pp. 93-94.

## Subtitle B. Efficient Management of Budget Authorities.

*Sec. 110. Intelligence Community Management Account.*

Section 110 authorizes appropriations for the Community Management Account (CMA) of the Director of National Intelligence (DNI) for fiscal year 2008.

Section 110 eliminates a provision from recent intelligence authorization legislation which limits the term of non-reimbursable details to the Office of the DNI (ODNI) to one year or less. Because the Intelligence Reform and Terrorism Prevention Act of 2004 provided the DNI with considerable flexibility to manage human resources, the old Community Management restriction regarding nonreimbursable details is too limiting. Instead, section 126 would provide for a term, not to exceed three years, of non-reimbursable details to the ODNI. The one year restriction was changed because it unduly restricts the ODNI's ability to facilitate the rotation of Intelligence Community employees, especially those on joint duty assignments.

Subsection (a) authorizes appropriations of $705,376,000 for fiscal year 2008 for the activities of the CMA of the DNI. Subsection (a) also authorizes funds identified for advanced research and development to remain available for two years.

Subsection (b) authorizes additional appropriations for the CMA as specified in the classified Schedule of Authorizations and permits the additional funding amount to remain available through September 30, 2008, except for funds for research and development activities, which remain available through September 30, 2009.

*Sec. 111. Authorization of Appropriations.*

Section 111 authorizes appropriations in the amount of $262,500,000 for fiscal year 2008 for the Central Intelligence Agency Retirement and Disability Fund.

Section 111 supports Enterprise Objective 10 (EO10) of the ODNI's National Intelligence Strategy, "Eliminate redundancy and programs that add little or no value and re-direct savings to existing and emerging national security priorities." In particular, Section 111 would update CIA financial management processes – one of the goals identified in EO10 – by providing the necessary funds in accordance with the responsibility of the Director of the CIA specified in Section 261(a) of the Central Intelligence Agency Retirement Act (50 U.S.C. 2091(a)).

*Sec. 112. Modification of availability of funds for different intelligence activities.*

Section 112 replaces the "unforeseen requirements" standard that governs reprogrammings of funds which is set forth in section 504(a)(3)(B) of the National Security Act, with a more precise standard consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The new standard would enhance the flexibility and capability of intelligence agencies to reprogram funds to meet higher-priority mission requirements.

Section 112 conforms the text of section 504(a)(3)(B) of the National Security Act of 1947 (50 U.S.C. 414(a)(3)(B) (governing the funding of intelligence activities)) with the more substantive text provided in Section 1011(a) of the Intelligence Reform and Terrorism Prevention Act of 2004(Pub.L. No. 108-458 (Dec. 17, 2004)) (governing the transfer and reprogramming by the Director of National Intelligence (DNI) of certain intelligence funding). This conforming amendment replaces the "unforeseen requirements" standard set forth in section 504(a)(3)(B) of the National Security Act with a clearer standard to govern reprogrammings of funds authorized for a different intelligence or intelligence-related activity.

Under this new standard, a reprogramming would be authorized if, in addition to the other requirements of section 504(a)(3), the new use of funds would "support an emergent need, improve program effectiveness, or increase efficiency." This modification brings the standard for reprogrammings of intelligence funding into conformity with the standards applicable to reprogrammings and transfers under section 102A(d) of the National Security Act of 1947. The modification preserves congressional oversight of proposed reprogrammings and transfers while enhancing the Intelligence Community's ability to carry out missions and functions vital to national security.

Section 112 supports Enterprise Objective 10 (EO10) of the ODNI's National Intelligence Strategy, "Eliminate redundancy and programs that add little or no value and re-direct savings to existing and emerging national security priorities." In particular, section 112 would improve the Intelligence Community's ability to align and reallocate resources to the highest priorities and strengthen the linkages between strategy, priorities, performance, and

investment -- two of the goals identified in EO10 -- by conforming section 504(a)(3)(B) of the National Security Act with the standard set forth in section 1011(a) of the IRTPA, thereby improving the Intelligence Community’s ability to reprogram funds to pursue higher-priority missions and activities vital to national security.

*Sec. 113. Increase in Employee Compensation and Benefits Authorized by Law.*

Section 113 provides that funds authorized to be appropriated by this Act for salary, pay, retirement and other benefits for federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in such compensation or benefits authorized by law.

*Sec. 114. Reserve for Contingencies of the Director of National Intelligence.*

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) strengthened the authorities of the Director of National Intelligence (DNI) to determine, oversee, and implement the National Intelligence Program (NIP). These new authorities are central to formulate the budget, advance Intelligence Community (IC) integration, improve coordination, and strengthen national intelligence capabilities.

Section 114 augments these authorities and creates an account, or "reserve" of funds, for the Director of National Intelligence (DNI) to use across the Intelligence Community to address emergency requirements, operational exigencies, and opportunities that arise outside the budget formulation cycle and cannot be addressed in a timely fashion through existing budgetary processes. Section 114 provides the DNI with the necessary budgetary and operational flexibility to lead a more agile organization that is more responsive to unanticipated IC requirements.

The section 114 reserve is limited to funds appropriated to the NIP in the RDT&E (research, development, test, and evaluation) appropriation from the Community Management Account, amounts which ordinarily are available for two fiscal years. The annual appropriation to the reserve cannot exceed $50 million in any fiscal year. Funds remain available as originally appropriated, after which any expired unused funds are returned to the Treasury.

Section 114 reserve funds are available to the DNI and IC elements for purposes permitted by law and consistent with regulations and guidance promulgated by the Office of the Director of National Intelligence (ODNI). The ODNI anticipates developing procedures similar to those currently established for management of the Central Intelligence Agency's (CIA's) Reserve for Contingencies. The ODNI will approve the use of the funds, the Office of Management and Budget OMB will approve their release from the reserve, and ODNI will notify Congress as required.

In addition, reserve funds are available for a program or activity not previously authorized by Congress when the ODNI has notified the congressional intelligence committees

of the intent to use such amounts for such a purpose, and fifteen calendar days have elapsed from such notification.

Moreover, with respect to intelligence activities and covert actions, and consistent with sections 413a and 413b of the National Security Act of 1947, as amended (50 U.S.C. sections 502 and 503), section 114 reserve funds are available for such undertakings only after the DNI has notified the appropriate congressional intelligence committee members of the intent to make such amounts available for such an activity.

Finally, a similar reserve for contingencies has been available to the Central Intelligence Agency (CIA) since the Agency's creation. The CIA reserve account permitted the former Director of Central Intelligence, and now the Director of the CIA, to transfer funds, with appropriate notification to Congress, to address significant intelligence requirements that arise during a fiscal year and that must be addressed outside the normal budget process. The CIA reserve has proven crucial to providing the CIA with the flexibility required to address contingencies as they arise. The new section 114 authority provides similar flexibility to the DNI.

Sec. 117. Multiyear National Intelligence Program

Section 117 updates the “multiyear national intelligence program” provision to incorporate and reflect organizational and nomenclature changes made by the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458).

*Sec. 118. References to Military Intelligence Program and Related Activities.*

Until FY 2007, the Defense Department's intelligence efforts were funded through the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA). The Defense Department since has abandoned these resource structures in favor of the new Military Intelligence Program (MIP), which is designed to ensure that the Defense Department, the Director of National Intelligence (DNI), and the Congress each has the transparency and insight required to assess the allocation of resources to meet Defense intelligence requirements.

The Intelligence Reform and Terrorism Prevention Act included participation of the DNI in the development of the annual JMIP and TIARA budgets, and the requirement for Secretary of Defense consultation with the DNI prior to transfer or reprogramming of JMIP funds. The new text that appears in section 118 changes the references from JMIP and TIARA to the new MIP.

*Sec. 120. Conferences Conducted by Elements of the Intelligence Community: Collection of Fees to Cover Costs.*

Section 120 authorizes Intelligence Community (IC) elements to charge fees to cover the costs of conferences and similar events that further the IC mission.

Outreach and interaction with academia, industry, and the public are important to the missions of IC elements. Through such activities, the IC shares its knowledge and draws on the expertise of academia and the private sector to improve its own activities and operations. One of the most efficient means by which to facilitate this exchange is through agency-sponsored conferences. Such conferences bring together large numbers of people in a setting that encourages the exchange of views and networking, and also allows participants to share best practices. Unfortunately, the ability of IC elements to host such conferences is limited by the inability of IC elements to charge a fee to cover the costs of such events. Section 120 resolves this problem by authorizing IC elements to charge fees to cover the costs of certain events.

Section 120 supports Enterprise Objective 1 (EO1), of the DNI's National Intelligence Strategy, "Build an integrated intelligence capability to address threats to the homeland, consistent with US laws and the protection of privacy and civil liberties." By facilitating IC conferencing activities, section 120 addresses the EO1 goal of building an integrated intelligence capability to address threats to the homeland by ensuring that IC elements are able to bring together members of the public and private sectors with IC staff to exchange information and develop innovative mechanisms for working together.

## Subtitle C. Modernizing Civilian Personnel Systems within the Intelligence Community.

*Sec. 121 . Enhancing Personnel Flexibilities Throughout the Intelligence Community.*

The Intelligence Reform and Terrorism Prevention Act of 2004 directed the Director of National Intelligence to prescribe personnel policies and programs for the Intelligence Community to enhance integration and to build a sense of cohesiveness within the Intelligence Community. With the development of the Intelligence Community's (IC) *Five Year Strategic Human Capital Plan and the release of the 100 Day Plan,* the Director of National Intelligence (DNI) has signaled a clear emphasis on IC personnel practices. In particular, the DNI wants to manage all of the intelligence elements as a single cohesive community. In support of this strategic plan, the DNI needs to have consistent enhanced personnel flexibilities across the entire IC. Section 121 amends subsection 102A of the National Security Act of 1947 to grant the DNI personnel authorities in several key areas.

Subsection 102A (t) allows the DNI, with the concurrence of the relevant Department head, to bring into the "excepted civil service all of the IC civilian elements that are not already in it. Because of their unique intelligence, investigative, and national security missions (with their attendant secrecy and security requirements), most elements of the IC are in the "excepted" civil service and thus exempt from the requirements of the "competitive" civil service regarding the appointment, assignment, promotion, demotion, and removal of civilian employees. However, the civilian employees of several IC elements (Department of State's Bureau of Intelligence and Research, Department of Energy/IN, Department of Treasury/IA, Department of Homeland Security/IA and the United States Coast Guard, The Department of Justice, and the Drug Enforcement Agency) are still covered under the competitive service rules. Those rules do not adequately take into account the IC's stringent security clearance requirements, or the need for secrecy with respect to organizational size, missions and functions, and the needs of these IC elements to have agile and responsive systems to hire employees, reassign employees, and—when necessary—remove unsuitable employees Specifically, this provision authorizes the DNI, with the concurrence of the head of the

department or agency concerned, and in coordination with the Office of Personnel Management (OPM), to convert existing competitive service positions in elements of the IC to excepted service positions. Moreover, at the request of the DNI, the heads of departments or agencies may establish new "excepted" service positions, if the DNI determines that these positions are necessary to carry out the intelligence functions of such elements of the IC. Section 121 also authorizes the DNI to establish the position classification and rates of basic pay for such positions. This subsection further authorizes the heads of the departments or agencies concerned to appoint individuals in such positions in the excepted service that were converted or created and to fix the compensation for such individuals within the applicable rates of basic pay established by the DNI.

Subsection 102A (u) provides enhanced pay authority for critical positions in the IC as to which such authority does not already exist. The DNI can authorize heads of agencies containing elements of the IC to fix the rate of basic pay for positions which require an extremely high level of expertise and which are critical to the accomplishment of an important mission. Rates of pay in excess of level II of the Executive Schedule would require the approval of the DNI; rates of pay in excess of level I of the Executive Schedule would require the approval of the President, or approval as otherwise authorized by law. This authority is similar to that given to the Director of OPM to fix the rates of pay for critical positions under 5 U.S.C. 5377.

Subsection 102A (v) grants broad authority to the DNI to authorize elements of the IC, with the concurrence of the head of the department or agency concerned and in coordination with the Director of OPM (for those matters that fall under the responsibilities of OPM under statute or executive order), to adopt compensation, performance management, and scholarship authority that have been authorized for any other element of the IC if the DNI determines that such adoption would improve the management and performance of the IC. The DNI would be required to notify the congressional intelligence committees at least 60 days before any such adopted authority is to take effect. For the purpose of this subsection, the term 'in coordination with the Director of OPM' means the Director of OPM will be provided a reasonable opportunity to review

and comment on a proposal to authorize the adoption of a compensation authority in another element of the IC. The DNI will take the comments of the Director of OPM into account and provide him or her with reasonable advance notice of the final decision and planned effective date of that decision. In the case of objections by the Director of OPM to a proposal that affects the coverage of employees under provisions of law administered by OPM, the DNI will not proceed with adoption of the proposal for such employees until the disagreement is resolved within the Administration.

ODNI and OPM intend to work collaboratively under these new authorities to further the DNI's statutory authority and responsibility to prescribe personnel policies and programs that encourage and facilitate joint assignments; to set standards for education, training and career development; to encourage and facilitate recruitment; and to promote diversity within the IC.

*Sec. 125. Contributions to Thrift Savings Plan.*

Section 125 would permit employees, including employees of elements the Intelligence Community, who make contributions to the Thrift Savings Fund out of basic pay to also make an advance election to contribute all or any part of any payment, other than basic pay, to the Fund. These additional contributions would not be subject to a matching employer contribution.

Section 125 would, effective at the time prescribed in regulations issued by the Executive Director of the Federal Retirement Thrift Investment Board in consultation with the Director of the Office of Personnel Management, amend sections 8351(d) and 8432(k) of Title 5, United States Code, to permit Federal employees to contribute to their Thrift Savings Plan (TSP) accounts any payment, other than basic pay, as may be prescribed by regulation. In addition, section 125 would repeal similar but more limited provisions that previously permitted certain Central Intelligence Agency employees to make direct payments to TSP under a now obsolete CIA personnel pilot program.

Generally, under current law, Federal employees can only contribute basic pay to their Thrift Savings plans, but not bonus or award monies. Authorizing contributions of bonus or award monies will permit employees to take full advantage of their ability to contribute to their Thrift Savings plans, consistent with existing limitations on the amount of contributions to certain retirement accounts. However, due to the operational complexities of such contributions, this provision provides for the issuance of necessary regulations by the Executive Director.

In this regard, a major complexity is that there is often no advance notice of such payments to employees, thus necessitating that contingent elections need to be made in advance. Further, provisions need to be made so that employees are aware of the annual limits of the Internal Revenue Code, and can make their election in such manner so as to avoid the problem of exhausting their annual transfer limit prematurely so as to lose potential agency matching payments under FERS.

*Sec. 126. Repeal of Restriction on the Use of Non-reimbursable Detailees.*

Section 126 does not include a provision present in recent intelligence authorization bills that limit the term of non-reimbursable details to the ODNI to one year or less. This restriction unduly restricts the ODNI's staffing ability and its ability to facilitate the rotation of IC employees, especially those on joint duty assignments. This section supports the objectives of the Strategic Plan of the Director of National Intelligence.

Section 126 parallels section 110 that omits language found in each recent Intelligence Authorization Acts that limits the term of non-reimbursable details to the ODNI to one year or less. Section 126 provides permanent authorization for details on a reimbursable or non-reimbursable basis from an element of the Intelligence Community to the staff of an element of the IC funded through the Community Management Account, that is, the ODNI. Such details will be determined under terms jointly agreed to by the DNI and the head of the sending department or agency, but the terms shall be no longer than three years. This authority will provide flexibility for the ODNI to receive support from other elements of the IC on a non-reimbursable basis for community-wide activities where both the sending agency and the ODNI would benefit from the detail.

## TITLE II – THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND INTELLIGENCE COMMUNITY MATTERS.

*Sec. 201. Federal Advisory Committee Act.*

Congress enacted the Federal Advisory Committee Act (FACA) (5 U.S.C. App. 2) to regulate the use of advisory committees throughout the Federal Government. FACA sets forth the responsibilities of Congress and the Executive Branch with regard to such committees and outlines procedures and requirements for such committees.

For example, under FACA, Federal agencies sponsoring advisory committees ordinarily open advisory committee meetings to the public, and, subject to the Freedom of Information Act, make available for public inspection papers and records, including detailed minutes of each meeting. For advisory committees handling extremely sensitive material, such openness requirements may be inconsistent with national security or business confidentiality requirements.

Therefore, FACA, as originally enacted in 1972, expressly exempted advisory committees used by the Central Intelligence Agency (CIA) and the Federal Reserve System, *see* 5 U.S.C. App. 2, section 4(b). Section 201 amends FACA to extend this exemption explicitly to those advisory committees established or used by the Office of Director of National Intelligence (ODNI).

*Sec. 202. Clarification of the Restriction against Co-Location of Office of Director of National Intelligence Headquarters*

Section 202 clarifies that the ban on co-location of the Office of the Director of National Intelligence (ODNI) with any other Intelligence Community (IC) element, which is slated to take effect on 1 October 2008, applies to the co-location of the headquarters of each. Section 202 also provides that the President may waive the ban if the President determines waiver is in the interests of national security, or if the President determines that the cost of providing for separate facilities is not warranted.

Section 202 affords flexibility to ensure that the ODNI or its various components may be located in the most appropriate facility or facilities. Because the ODNI handles some of the most sensitive intelligence information within the U.S. Government, it is important that the ODNI have the highest level of physical and technical security possible.

The ODNI intends to locate its headquarters where it is separate and apart from the headquarters of the various IC elements. However, considering the difficulty and cost of finding or building a facility that meets the appropriate physical and technical security standards, the President must have the discretion to locate any or all components of the ODNI in one or more existing IC facilities if doing so would be in the interests of the national security.

This provision would also authorize the President to waive the ban on co-location where the cost of providing separate facilities is unwarranted. This could be the case where is may be prudent or convenient for communications or logistical purposes to locate an element of the ODNI near the headquarters of another element of the intelligence community. If co-location would be a more cost-effective solution and if the additional cost of separate headquarters did not support the potential benefits of the limitation(such as avoiding any real or apparent confusion of the identity or authorities of the two entities), the President should have the authority to waive the ban on co-location.

*Sec. 203. Application of the Privacy Act to the Director of National Intelligence and the Office of Director of National Intelligence.*

Section 203 authorizes the Director of National Intelligence (DNI) to issue regulations to protect information in records systems of the Office of the DNI (ODNI) from otherwise mandated requirements under the Privacy Act of 1974 (5 U.S.C. section 552a), as amended. This authority, which is identical to that currently available to the Director of the Central Intelligence Agency (CIA), is necessary to ensure that the DNI may provide adequate and appropriate safeguards for certain sensitive information in ODNI records systems, and fulfill the ODNI mission.

Historically, the Privacy Act has included a long-standing provision by which the Director of the CIA could promulgate rules to exempt any system of records within the CIA from certain requirements under the Act. This provision was designed to ensure that the CIA could provide adequate and appropriate safeguards for certain sensitive information in its records systems.

The DNI, as the head of the Intelligence Community, requires the ability to safeguard sensitive information in records systems within the ODNI. The DNI, as the President’s principal intelligence advisor, has broad access to and responsibility for analyzing and disseminating national intelligence for national security purposes. Whereas the CIA has a collection mission that the DNI does not, the DNI has expanded authorities and responsibilities for accessing and analyzing all-source intelligence -- authorities and responsibilities that mirror and in many cases go far beyond those previously afforded the CIA.

The ODNI is committed to the protection of privacy and civil liberties, and has mechanisms for protecting those concerns, including the Civil Liberties Protection Office and access to the Privacy and Civil Liberties Oversight Board. Like the CIA, ODNI will continue to remain subject to important provisions of the Privacy Act.

Section 203 amends the Privacy Act, 5 U.S.C. section 552a(j) to extend to the DNI the authority to promulgate

rules by which certain records systems of the ODNI may be exempted from certain Privacy Act requirements.

*Sec. 205. PROTECTION OF CERTAIN FILES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE*.

Section 205 adds a new section 706 to the National Security Act of 1947, to exempt specific categories of Office of the DNI (ODNI) files from the search, review, and disclosure provisions of the Freedom of Information Act (FOIA) (5 U.S.C. 552). This exemption parallels and reinforces the statutory operational files FOIA exemptions already granted to five of the main Intelligence Community elements: the Central Intelligence Agency (CIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA). The exemption provided by new section 310 preserves the statutory framework for existing operational files exemptions and removes any uncertainty about whether those exemptions are lost by sharing the sensitive information contained in such files with the ODNI.

In order to carry out the authorized duties and responsibilities of the DNI under section 102A of the National Security Act of 1947, as amended, the ODNI will receive intelligence and intelligence-related information from existing operational files, and create new records that include or use such information. The ODNI has received, and will expect to continue to receive, broad FOIA requests for intelligence community documents that would require a search of such operational files within the ODNI. ODNI-received 'operational files' information, and ODNI material that includes or is derived from existing 'operational files' information, warrants the same search, review and disclosure exemption under FOIA as the same sensitive information in CIA, NGA, NRO, NSA and DIA operational files. (See, National Security Act of 1947, as amended,§§ 701-705, 50 U.S.C. 431,432,432a,432b and 432c.) Furthermore, the 'operational files' in the originating agency should not lose their exemption as a result of providing records from those files to the ODNI.

In order to maintain the nexus between exempt operational files created in the ODNI with the originating exempt operational files, this provision contains a requirement that the operational files created in the ODNI "shall be similar in nature to the originating operational files from which the record was disseminated or provided, as such files are defined in Title VII of this Act." The

DNI will promulgate regulations to implement this authority within the ODNI.

Section 205 supports Enterprise Objective 7 (EO7) of the ODNI's National Intelligence Strategy, "Create clear, uniform security practices and rules that allow us to work together, protect our nation's secrets and enable aggressive counterintelligence activities." In particular, Section 310 supports the underlying goals of EO7 by preserving the existing operational files exemptions of the relevant elements of the intelligence community and clarifying the effects on these exemptions of sharing information with the Office of the Director of National Intelligence.

*Sec. 206. Strengthening Access to Information.*

Section 206 provides statutory authority for the Director of National intelligence (DNI) to use National Intelligence Program (NIP) funds to quickly address deficiencies or requirements that arise in intelligence information sharing capabilities related to intelligence mission responsibilities.

Section 206 adds a new section 102A(g)(1)(G) to the National Security Act of 1947 that gives clear authority to the DNI to provide – and clear authority to a receiving agency or component to accept and use – appropriately authorized and appropriated funds, services, or equipment that address intelligence information sharing requirements, even or especially if the requirements arise outside the normal budget or requirements cycle.

Moreover, section 206 specifically gives the DNI the authority, not found in Section 102A(d) of the National Security Act, to provide funds to non-NIP activities for the purpose of addressing critical gaps in intelligence information sharing capabilities. Without this authority, the development and implementation of necessary intelligence information sharing capabilities could be delayed due to an agency's lack of authority to accept or use such DNI-funded systems, lack of current-year funding, or augmentation of appropriations concerns.

Section 206 also is important to the development and deployment of systems of common concern that are designed to enhance the collection, processing, analysis, exploitation, and dissemination of national intelligence -- systems will greatly benefit the Intelligence Community. Intelligence information sharing systems must be interconnected, interoperable, secure, and available: Section 206, by permitting the DNI to help find funding for such systems, will help ensure their development. In addition, establishing standards for the utilization and operation of such systems is consistent with DNI authorities set forth in the IRTPA, including section 1018.

Finally, the proposed section 206 authority is similar to authority granted to the National Geospatial-Intelligence Agency with respect to imagery and imagery-related systems.

*Sec. 207. Application of Certain Financial Reporting Requirements to Director of National Intelligence.*

Section 207 delays the applicability to the Director of National Intelligence (DNI) of the audited financial reporting requirements of 31 U.S.C. section 3515. This grace period gives the DNI the necessary time to establish a financial management system for the Office of the DNI (ODNI) that can generate financial statements to meet the prescribed legal and audit standards.

Ordinarily, section 3515 requires certain Federal agencies, including the ODNI, to prepare and submit to the Congress and the Director of the Office of Management and Budget (D/OMB), not later than 1 March of each year, an audited financial statement for the preceding fiscal year. The Accountability of Tax Dollars Act of 2002, Public Law 107-289, amended 31 U.S.C. section 3515, and gave the D/OMB the authority to waive the audited financial reporting requirements for up to two fiscal years for any newly covered Executive agency. Section 3515 subsequently was amended to permit the D/OMB to waive the reporting requirements for a covered agency if the budget authority for that agency did not exceed $25 million in the given fiscal year and if the D/OMB determined that there was an absence of risk associated with the agency's operations. The D/OMB cannot use this limited waiver authority to grant a grace period to the ODNI. Therefore, section 207 would exempt the ODNI from the requirements of section 3515 for fiscal years 2008, and 2009.

The former Community Management Staff (CMS) took significant strides to address financial management issues, and section 207 will permit the DNI adequate time to complete CMS' diligent efforts to establish an ODNI financial management system. This system is critical to the ODNI's generation of audited financial statements that satisfy generally accepted accounting principles, applicable laws, and financial regulations.

*Sec. 208. Protection of Intelligence Sources and Methods From Unauthorized Disclosure.*

Section 208 increases the flexibility of the Director of National Intelligence (DNI) to carry out the authority and responsibility to protect intelligence sources and methods from unauthorized disclosure, by striking the restriction on delegation of that authority by the DNI. This change makes the provision for DNI protection of intelligence sources and methods parallel to the prior National Security Act provision that had vested the power in the former Director of Central Intelligence (DCI) and that did not constrain the DCI from delegating the authority. *See* old section 103(c)(7); 50 U.S.C. section 403-3(c)(7) prior to IRTPA amendments).

*Sec. 209. Program Manager for the Information Sharing Environment and the Information Sharing Council.*

Section 209 amends subsection 1016(f) and (g) of the Intelligence Reform and Terrorism Prevention Act of 2004 to amend and fix the terms of the Program Manager for the Information Sharing Environment (ISE), and the Information Sharing Council, to reflect the requirement for continued and effective management and implementation of the ISE beyond the two-year period provided for in section 1016, as contemplated in the Implementation Plan for the Information Sharing Environment, approved by the President.

*Sec. 214. Membership of the Director of National Intelligence on the Transportation Security Oversight Board*

Section 214 substitutes the Director of National Intelligence (DNI) or the DNI's designee as a member of the Transportation Oversight Board under 49 U.S.C. section 115(b)(1), in place of the Director of the Central Intelligence Agency (D/CIA) or the D/CIA's designee.

*Sec. 215. Technical Corrections to the National Security Act.*

Section 215 corrects several inadvertent technical anomalies in the National Security Act of 1947 arising from the amendments made to that Act by the Intelligence Reform and Terrorism Prevention Act of 2004.

The first correction clarifies that the funds referred to in section 102A(d)(3) of the National Security Act of 1947 are those noted in section 102A(d)(1)(A) of the Act (i.e., funds made available under the National Intelligence Program).

The second correction removes the extraneous reference to “personnel” in section 102A(d)(5)(A) of the National Security Act, as that Act was amended by the Intelligence Reform and Terrorism Prevention Act of 2004.
Section 102A(d) of the National Security Act addresses the transfer and reprogramming of funds by DNI, whereas section 102A(e) addresses the transfer of personnel by the DNI.

The third correction clarifies that the regulations that the DNI may issue under section 102A(l)(2)(B) of the National Security Act are regulations to carry out the promotion rate provisions in section 102A(l)(2)(A) of the Act.

The forth correction deletes an erroneous cross-reference to the ‘dispute resolution’ subsection of section 119 of the National Security Act and substitutes the intended cross-reference to the ‘Directorate of Intelligence’ subsection of section 119.

*Sec. 216. Technical Corrections to Intelligence Reform and Terrorism Prevention Act of 2004.*

Section 216 corrects a number of inadvertent technical errors in the specified sections of Public Law 108-458.

*Sec. 218. Repeal of Certain Authorities relating to the Office of the National Counterintelligence Executive.*

Section 218 makes technical corrections to eliminate certain independent administrative authorities that had been vested in the National Counterintelligence Executive (NCIX) when that official was appointed by and reported to the President. Those authorities are unnecessary, redundant, and anomalous, and could or would undercut the authorities of the Director of National Intelligence (DNI), now that the NCIX is to be appointed by and under the authority, direction, and control of the DNI.

*Sec. 219. Technical Corrections to Executive Schedule*

Section 219 makes several technical corrections to the Executive Schedule. This section clarifies that the position of the Director of the Central Intelligence Agency (D/CIA) is at Level II of the Executive Schedule. It is, of course, the case that section 1081 of the Intelligence Reform and Terrorism Prevention Act of 2004, when read in conjunction with section 1015 of that Act, has the legal effect of substituting the "Director of the Central Intelligence Agency" for the previous reference in 5 U.S.C. 5313 to "Director of Central Intelligence". This amendment reinforces that the D/CIA is an Executive Schedule Level II position, and removes the need to track and trace through multiple other provisions to reach that conclusion. Section 219 also strikes the outdated references to the Deputy Directors of Central Intelligence in 5 U.S.C. 5314, and corrects the erroneous reference to the "General Counsel to the National Intelligence Director" in 5 U.S.C. 5315.

Section 219 supports Enterprise Objective 4 (EO4), "The U.S. Intelligence Community's Strategic Human Capital Plan." In particular, section 219 supports the underlying goals of EO4 by updating the law to clearly reflect changes in titles of leadership positions in the Central Intelligence Agency.

## TITLE III – MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY.

### Subtitle A. Central Intelligence Agency

*Sec. 301. Report on Audited Financial Statements Progress*

Section 301 repeals the requirement that the Director of the Central Intelligence Agency (D/CIA) submit to the Congressional intelligence committees an annual report describing the activities being undertaken to ensure that financial statements of the CIA can be audited in accordance with applicable law and requirements of the Office of Management and Budget. The report is unnecessary and duplicative now that CIA has submitted and will continue to submit audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002, Public Law 107-289 and 31 U.S.C. 3515.

Section 301 supports Enterprise Objective 10 (EO10) of the ODNI's National Intelligence Strategy, "Eliminate redundancy and programs that add little or no value and re-direct savings to existing and emerging national security priorities." In particular, section 301 would streamline CIA financial management processes – one of the goals identified in EO10 – by eliminating the requirement for a redundant annual report.

*Sec. 302. Additional Functions and Authorities for Protective Personnel at the Central Intelligence Agency.*

Section 302 amends section 5(a)(4) of the Central Intelligence Agency (CIA) Act of 1949 (50 U.S.C. section 403f(a)(4)) which authorizes protective functions by designated security personnel who serve on CIA protective details.

This section authorizes protective detail personnel, when engaged in the performance of protective functions, to make arrests in two circumstances. First, CIA protective detail personnel may make arrests without a warrant for any offense against the United States, regardless of whether it is a felony, misdemeanor, or infraction, that is committed in their presence. Second, protective detail personnel also may make arrests without a warrant if they have reasonable grounds to believe that the person to be arrested has committed or is committing a felony, but not other offenses, under the laws of the United States.

Regulations approved by the Director of the CIA and the Attorney General will provide safeguards and procedures to ensure the proper exercise of this authority; however, the provision specifically does not grant any authority to serve civil process or investigate crimes.

By granting CIA protective detail personnel limited arrest authority, this provision mirrors statutes applicable to other Federal law enforcement agencies authorized to perform protective functions. The authority provided under this section is consistent with those of other Federal elements with protective functions, such as the Secret Service (*see* 18 U.S.C. section 3056(c)(1)(c)), the State Department's Diplomatic Security Service (*see* 22 U.S.C. section 2709(a)(5)), and the Capitol Police (*see* 2 U.S.C. section 1966(c)).

Arrest authority will contribute significantly to the ability of CIA protective detail personnel to fulfill their responsibilities to protect officials against serious threats without being dependent on the response of Federal, State, or local law enforcement officers. The grant of arrest authority under this amendment is supplemental to all other authority that CIA protective detail personnel have by virtue of their statutory responsibility to perform the protective functions set forth in the CIA Act of 1949.

In addition, this section also authorizes the Director of the CIA, on the request of the Director of National Intelligence (DNI), to make CIA protective detail personnel available to the DNI. The DNI, in consultation with the Director of the CIA and the Attorney General, will advise the intelligence committees within 180 days of enactment of this Act whether this arrangement meets the protective requirements of the ODNI or whether other statutory authority is necessary.

Finally, although this bill currently provides separate authorities for CIA and NSA protective details, in the future the DNI may advise the intelligence committees that overall policies, procedures, and authorities be provided to protective services for other Intelligence Community elements, personnel and/or their immediate families.

Section 302 supports Enterprise Objective 7 (EO7), of the ODNI's National Intelligence Strategy, "Create clear, uniform security practices and rules that allow us to work together, protect our nation's secrets and enable aggressive counterintelligence activities." By providing the CIA protective detail personnel a limited detention and arrest authority and authorizing their availability to support the DNI and other personnel within the ODNI, section 302 properly responds to the EO7 goals of improving the Intelligence Community's physical security programs to better support the DNI's mission and effectively respond to evolving critical threats through proactive and integrated security practices.

*Sec. 303. Deputy Director of the Central Intelligence Agency*

Section 303 adds provisions to the National Security Act that establish in statute the position of Deputy Director of the Central Intelligence Agency (DD/CIA), specify that the President appoints the DD/CIA, specify the duties and status of the DD/CIA, and place the position of DD/CIA at Level III of the Executive Schedule. Section 303 includes a provision that directs when the amendments shall become effective.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) separated the leadership of the Intelligence Community (IC) from the leadership of the CIA. Although the IRTPA explicitly provided for a Director of the CIA, it did not provide for a statutory deputy to the Director. Section 303 resolves this issue and establishes the position of the DD/CIA.

Section 303 supports Enterprise Objective 4 (EO4) of the ODNI's National Intelligence Strategy, "Attract, engage, and unify an innovative and result-focused Intelligence Community workforce." In particular, Section 303 provides for enhanced leadership – one of the goals identified in EO4 – by creating a statutory Deputy Director of the CIA vested with statutory authority to act for, and exercise the powers of, the Director of the CIA in the event the Director is absent or disabled or the position of Director of the CIA is vacant.

*Sec. 304. Technical Amendments Relating to Titles of Central Intelligence Agency Positions.*

Section 304 corrects outdated references to the Executive Director, Deputy Director for Operations, and Deputy Director for Administration in section 17(d)(3)(B)(ii) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q(d)(3)(B)(ii)). The technical amendments of this section reflect the recent changes of the position titles of the Executive Director to Associate Deputy Director, the Deputy Director for Operations to Director of the National Clandestine Service, and the Deputy Director for Administration to Director for Support.

Section 304 supports Enterprise Objective 4 (EO4), of "The U.S. Intelligence Community's Strategic Human Capital Plan." By updating the law to reflect the correct titles of certain leadership positions within Central Intelligence Agency's current organizational structure, Section 304 promotes the EO4 goal to create a culture of leadership at all levels by supporting a new leadership blueprint aimed at an integrated Intelligence Community culture that values service, integrity, and accountability.

*Sec. 305. General Counsel of the Central Intelligence Agency.*

Section 305 changes the appointment process for the General Counsel of the Central Intelligence Agency. Section 305 provides for appointment of the General Counsel of the CIA by the President, and removes the current requirement that the CIA General Counsel be confirmed by the Senate.

The amendment introduced by section 305 accomplishes several goals. It reduces the number of positions in the Intelligence Community that require Senate confirmation, expedites the process of filling vacancies in the very important and sensitive position of General Counsel of the CIA, yet appropriately ensures that appointments to the position are considered and made at the very highest level of the Executive Branch. Section 305 preserves the CIA General Counsel position as one to which Level IV of the Executive Schedule applies, and therefore does not amend section 5315 of title 5, United States Code.

Section 305 supports Enterprise Objective 4 (EO4) of the ODNI's National Intelligence Strategy, "Attract, engage, and unify an innovative and result-focused Intelligence Community workforce." In particular, Section 305 provides for enhanced leadership – one of the goals identified in EO4 – by enabling the General Counsel position to be filled more readily so that the Agency may more expeditiously utilize the expertise of the General Counsel in addressing pressing and sensitive legal issues.

*Sec. 306. Section 5(a)(1) of the Central Intelligence Agency Act of 1949.*

Section 306 amends section 5(a)(1) of the Central Intelligence Agency Act of 1949 (CIA Act) by striking outdated references to the National Security Act of 1947 and broadening the section's applicability to include any CIA functions or activities authorized by law. The Intelligence Reform and Terrorism Prevention Act of 2004 significantly restructured and renumbered multiple sections of the National Security Act of 1947, leaving references in section 5(a)(1) of the CIA Act to provisions that no longer exist as such or are otherwise no longer pertinent.

Section 306 eliminates those references and adopts a broader standard of Agency functions or activities that are authorized by law. This change not only broadens the section for CIA purposes but also broadens its applicability for the Director of National Intelligence, who is authorized by section 102A(n) of the National Security Act of 1947 (50 U.S.C. 403-1(n)) to exercise the so-called appropriations authorities referred to in the CIA Act.

Section 306 supports Enterprise Objective 10 (EO10) of the ODNI's National Intelligence Strategy, "Eliminate redundancy and programs that add little or no value and re-direct savings to existing and emerging national security priorities." In particular, Section 306 would update and improve CIA and ODNI financial management processes – one of the goals identified in EO10 – by updating and broadening the standard of functions authorized by law so that the Agency and the ODNI may more fully utilize their respective authorities.

*Sec. 308. Travel on Any Common Carrier for Certain Intelligence Collection Personnel*

Section 308 authorizes the Director of the Central Intelligence Agency (CIA), with respect to CIA employees, to delegate the specified travel-related authority.

Section 308 supports Enterprise Objective 3 (EO3) of the ODNI's National Intelligence Strategy, "Re-balance, integrate, and optimize collection capabilities to meet current and future customer and analytic priorities." In particular, section 308 optimizes the integration and responsiveness of the collection enterprise by providing greater flexibility in meeting collection demands.

*Sec. 313. Exclusion of Gain from Sale of a Principal Residence by Certain Employees of the Intelligence Community.*

Section 313 amends Section 121(d(9)) of the Internal Revenue Code (relating to exclusion of gain from sale of principal residence) to permit certain officers and employees of the Intelligence Community serving in domestic locations to elect to suspend for a maximum of 10 years the five-year test period for ownership and use during certain absences.

Under present law, an eligible individual taxpayer may exclude up to $250,000 ($500,000 if married filing a joint return) of gain realized on the sale or exchange of a principal residence. To be eligible for the exclusion, the taxpayer generally must have owned and used the residence as a principal residence for at least two of the five years prior to the sale or exchange. A taxpayer who fails to meet these requirements by reason of a change of place of employment, health, or, to the extent provided by regulations, unforeseen circumstances, is able to exclude an amount equal to the fraction of the $250,000 ($500,000 if married filing a joint return) that is equal to the fraction of the two years that the ownership and use requirements are met.

Special rules relating to officers and employees of the Intelligence Community serving at duty locations outside of the United States were added last year by Public Law 109-432. These amendments exclude similarly situated employees of the Intelligence Community who serve on qualified extended duty at domestic stations outside of the Washington Metropolitan area. If an election is made under this amended provision, the five-year period ending on the date of the sale or exchange of a principal residence is extended up to ten years during which the taxpayer or the taxpayer’s spouse is on qualified official extended duty as an officer or employee of the Intelligence Community. The election may be made with respect to only one property for a suspension period.

Section 313 supports Enterprise Objective 4 (EO4) of the ODNI’s National Intelligence Strategy, “Attract, engage, and unify an innovative and result-focused Intelligence Community workforce.” In particular, Section 313 would help attract and retain the highest caliber

employees and further integrate the IC's "Total Force"– two of the goals identified in EO4 – by enabling Intelligence Community employees and officers serving on qualified extended duty at domestic stations outside of the Washington Metropolitan area to receive the same tax benefit as their counterparts serving at duty locations outside the United States.

Sec. 317. Technical Modifications to Mandatory Retirement Provision of Central Intelligence Agency Retirement Act.

Section 317 updates the Central Intelligence Agency Retirement Act provision on mandatory retirement to reflect the Agency's abolition of pay grades within the Senior Intelligence Service (SIS) and the Agency's adoption of SIS personal ranks. As part of the revised SIS program approved by the Director of Central Intelligence in February 2004, the Agency—effective 11 July 2004—adopted a single pay range for the SIS, thereby eliminating the six SIS pay grades. The CIA Executive Director subsequently approved an SIS personal rank structure comprising levels 1-6, effective 1 December 2005. The change made by Section 317 resolves the discrepancy between the prior version of Section 235(b)(1) of the CIA Retirement Act and the revised SIS structure by deleteting the reference to level of compensation in current law and replacing it with a reference to SIS rank,

Section 317 supports Enterprise Objective 4 (EO4) of the ODNI's National Intelligence Strategy, "Attract, engage, and unify an innovative and result-focused Intelligence Community workforce." Section 317 helps attract and retain the highest caliber employees by bringing the CIA Retirement Act and current retirement system up to date to reflect the current SIS structure.

## Subtitle B. Department of Defense

*Sec. 321. Enhancements to the National Security Agency Training Program.*

Section 321 amends the National Security Agency (NSA) Act of 1959. The amendment to section 16(d)(1)(C) clarifies that "termination of employment" includes situations where employees fail to maintain satisfactory academic performance as defined by the Director of the NSA. Such employees shall be in breach of their contractual agreement and, in lieu of any service obligation arising under such agreement, shall be liable for repayment. Failure to maintain satisfactory academic performance always has been grounds for default resulting in the right of the Government to recoup the educational costs expended for the benefit of the defaulting employee. Thus, the change to section 16(d)(1)(C) is not a substantive change, but rather a clarification.

Section 321 also amends the NSA Act by amending section 16(e), which currently requires NSA to publicly identify to educational institutions which students are NSA employees. Deletion of this disclosure requirement will enhance the ability of NSA to protect personnel and prospective personnel, and preserve the ability of training program participants to undertake future covert or other sensitive assignments for the intelligence community. At the same, however, it leaves intact the long-standing prohibition against participants in the training program engaging in any intelligence functions at the institutions they attend under the program. *See* H.R. Rep. 99-690, Part I (July 17, 1986) ("NSA employees attending an institution under the program will have no intelligence function whatever to perform at the institution.").

*Sec. 322. Additional Functions and Authorities for Protective Personnel of the National Security Agency.*

Section 322 amends the National Security Agency (NSA) Act of 1959 (50 U.S.C. section 402 note) by adding a new section 20, to clarify and enhance the authority of protective details of NSA.

After the 9/11 attacks, the Secretary of Defense designated the Director of the National Security Agency as a "high risk position." Under DoD regulations, executives in high risk positions warrant protective details. Since being designated as a "high risk position," the Director of NSA has had such a detail.

Because the Director's detail is established through DoD regulation that provides limited protective authority, the protective detail lacks key detention and arrest authority that would enable it to perform its job most effectively. (See DOD Handbook 0-2000.12-H, DOD Directive 2000.12, and DOD Instruction 2000.16). Provision of the additional protection authority by statute would ensure that the detail has the necessary authority to perform its job.

New section 20(a) would grant the NSA protective detail similar arrest and detention authority as held by State Department details and is the same as what the Administration is seeking for the CIA. Under this authority, the protective detail would be able to respond appropriately to threats or actual attacks against the NSA Director. In particular, protective detail personnel would be able to make arrests without a warrant for any offense against the United States, regardless of whether it is a felony, misdemeanor, or infraction, that is committed in their presence. Protective detail personnel would also be able to make arrests without a warrant if they have reasonable grounds to believe that the person to be arrested has committed or is committing a felony under the laws of the United States. The arrest authority for NSA protective detail personnel would be subject to guidelines approved by the Director of NSA and the Attorney General; however, the provision specifically does not grant any authority to serve civil process or investigate crimes.

Finally, although this bill currently provides separate authorities for CIA and NSA protective details, the DNI may advise the intelligence committees in the future that overall policies, procedures, and authorities should be provided to protective services for other Intelligence Community elements, personnel and/or their immediate families.

*Sec. 323. Technical Amendments for the National Geospatial-Intelligence Agency.*

Section 323 makes several technical changes to the United States Code and other laws to bring these provisions in line with the agency name change from the National Imagery and Mapping Agency to the National Geospatial-Intelligence Agency, as provided for in section 921(b) of the National Defense Authorization Act for Fiscal Year 2004 (Pub. L. 108-136, 117 Stat. 1568 (2003)).

**Subtitle C. Department of State; Department of Treasury; Federal Bureau of Investigation; Department of Homeland Security.**

*Sec. 354. Elimination of Reporting Requirement for the Department of Treasury.*

Section 354 proposes to eliminate the requirement in 50 USC subsection 404m(a) that the Department of the Treasury submit a semi-annual report to the congressional intelligence oversight committees on the U.S. Government's operations against terrorist financial networks. The Department of the Treasury asserts that this reporting requirement has served its purpose and become unnecessary for the reasons set forth below.

When section 342 of the Intelligence Authorization Act for Fiscal Year 2003 amended the National Security Act of 1947 with this reporting requirement, the Treasury Department was receiving little information about terrorist financing from other U.S. law enforcement and intelligence agencies. Congress attempted to remedy the situation by requiring other agencies to provide relevant terrorist financing information to the Treasury for inclusion in this report.

Since the creation of the Office of Intelligence and Analysis (OIA) in 2004, the Treasury Department has become far better integrated into the Intelligence Community (IC), and the Department has developed significantly closer ties with its law enforcement partners, rendering this report no longer necessary. OIA now has comprehensive arrangements with various intelligence, law enforcement, and military organizations, which have resulted in far greater information sharing and coordination. For example, OIA now works jointly with the Federal Bureau of Investigation (FBI), both at FBI Headquarters and field office levels, on terrorist financing investigations. In addition, during the past year, OIA has developed closer ties with the Central Intelligence Agency.

In 2005, OIA hired a full time Requirements Officer, who has increased Treasury's profile in the IC requirements process by aggressively delivering requirements and evaluations on behalf of all Treasury entities to the IC. In these requirements submissions, Treasury includes comprehensive background information, as well as detailed

statements of Treasury's intelligence gaps to help focus the IC on Treasury's requirements. In response to Treasury's detailed requests, the IC has increased its level of tailored support to Treasury, making this report unnecessary.

Treasury asserts that taken together, these developments have rendered the subsection 404m(a) report unnecessary. Therefore new section 354 proposes that the semiannual report required by 50 USC section 404m(a) be deleted. In addition, section 354 leaves intact the emergency notification provisions of section 404m(b), but with a different paragraph heading.

*Sec. 355. Clarifying amendments relating to Section 105 of the Intelligence Authorization Act for Fiscal Year 2004.*

Section 355 amends section 105 of the Intelligence Authorization Act for Fiscal Year 2004 (Pub.L. No. 108-177 (Dec. 13, 2003)) to refer to the Director of National Intelligence (DNI) rather than the former Director of Central Intelligence (DCI).

Initially, section 105 clarified that the establishment of the Office of Intelligence and Analysis within the Department of the Treasury and its reorganization within the Office of Terrorism and Financial Intelligence, did not affect the authorities and responsibilities of the DCI with respect to the Office of Intelligence and Analysis as an element of the Intelligence Community. *See* Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, section 105 (Dec. 13, 2003)) and Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, Pub. L. No. 108-447, Div. H, section 222 (Dec. 8, 2004). New section 355 updates section 105 to reflect the authorities and responsibilities of the DNI, and adds a cite.

*Sec. 360. Department of Homeland Security Information.*

Section 360 amends section 1405 of the John Warner National Defense Authorization Act for Fiscal Year 2007, (hereinafter "FY07 Defense Authorization Act") (Public Law 109-364), to make it consistent with the existing language and framework under section 892 of the Homeland Security Act of 2002 (6 USC section 482) and section 1016 of Intelligence Reform and Terrorism Prevention Act (6 USC section 485), and the authorities of the President, therein, concerning the treatment and sharing of homeland security information.

6 USC section 482 defines "homeland security information," and provides that homeland security information shared with a State or local government will remain "under the control" of the Federal agency that provided it and that no State or local disclosure laws could apply to that information once it was shared.

Section 1405 of the FY07 Defense Authorization Act amended title 10 and created a new section 130d to ensure that such information, though shared with State and local personnel who are involved in the prevention of or response to terrorist activity, does not become subject to disclosure under the Freedom of Information Act (5 U.S.C. 552) by virtue of such sharing. According to the new 10 USC section 130d,

> "Confidential business information and other sensitive but unclassified homeland security information <u>in the possession of the Department of Defense</u> that is shared, pursuant to section 892 of the Homeland Security Act of 2002 (6 U.S.C. 482), with State and local personnel (as defined in such section) shall not be subject to disclosure under section 552 of title 5 by virtue of the sharing of such information with such personnel." (emphasis added).

That is, under the new section 130d, "confidential business information and other sensitive but unclassified homeland security information" does not lose any of its protections or exemptions from disclosure under the FOIA simply because the information was shared with State and local personnel pursuant to 6 USC section 482. Unfortunately, this protection applies only to information in the possession of the Department of Defense.

Limiting this protection only to information that is "in the possession of the Department of Defense" could have harmful unforeseen consequences for intergovernmental information sharing and pose operational hardships and perhaps legal obstacles for other Federal agencies that also share homeland security information with State and local personnel.

To resolve the tension between the FY07 defense authorization section 1405 and the Homeland Security Act, DHS proposes five amendments to section 1405. First and foremost, section 1405 is amended so that it is applicable to *all* Federal agencies and not just the Department of Defense by amending the phrase, "in the possession of the Department of Defense," to refer to "any Federal agency." This amendment eliminates both the negative implications and potential operational distortions created by limiting the application of section 1405 only to the Defense Department.

Second, this amendment clarifies that applicable FOIA exemptions attached to confidential business or homeland security information are not waived merely because said information was shared with State and local personnel.[1]

Third, this amendment replaces the expression "other sensitive but unclassified homeland security information," with the expression, "Homeland security information." To the extent that section 1405 references information that already is defined by statute, it is best to reflect the language and terminology used in 6 USC section 482. For example, the use of the term "sensitive but unclassified homeland security information" does not appear in section 482, which refers only to "homeland security information."

Fourth, the section title is amended to reflect these changes.

Fifth, for consistency, a clerical amendment to the title 10 table of contents reflects this change.

[1] *See also Students Against Genocide v. Dep't of State*, 257 F.3d 828, 836 (D.C. Cir. 2001) (noting that, generally, the government may not rely on an otherwise valid exemption to justify withholding information that already has been officially released to the public).

*Sec. 361. Technical Amendment Relating to the Coast Guard Intelligence Element.*

Prior to the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA 2004) (Public Law 108-458), the intelligence element of the Coast Guard was an independent member of the intelligence community and, like the other intelligence elements of the armed forces, responsible for the full range of intelligence activity. National Security Act of 1947, § 3(4)(H) (50 U.S.C. § 401a(4)(H)).

The IRTPA 2004 amended the statutory definition of "intelligence community" and introduced a technical drafting error with regard to the reference to the intelligence element of the Coast Guard.

Sec. 361 would correct this drafting error by locating reference to the Coast Guard in the members of the intelligence community with the other uniformed services. This sec. 361 would amend the National Security Act as follows:

* * * * * * *

(4) The term "intelligence community" includes—

* * * * * * *

(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, **the Coast Guard,** the Federal Bureau of Investigation, and the Department of Energy.

* * * * * * *

(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information~~, including the Office of Intelligence of the Coast Guard~~.

## TITLE IV – MATTERS RELATING TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

*Sec. 400. Short title.*

This section sets forth the title of this portion of the bill as the ‘‘Foreign Intelligence Surveillance Modernization Act of 2007’’.

*Sec. 401. Definitions.*

Section 401 amends the definitions of several terms used in the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. 1801-1871).

Subsection 401(a) amends FISA's definition of "agent of a foreign power" to include non-U.S. persons who possess or receive significant foreign intelligence information while in the United States. This amendment fills a gap in FISA's current definition to address circumstances in which a foreign individual is known to have valuable foreign intelligence information, but the individual's relationship to a foreign power is unclear. Collection of information from such an individual would be subject to the approval of the Foreign Intelligence Surveillance Court (FISC).

Subsection 401(b) also amends FISA's definition of "electronic surveillance." When FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress intended to exclude from FISA's scope. Subsection 401(b) provides a new, technologically neutral definition of "electronic surveillance" focused on the core question of who is the subject of the surveillance, rather than on how or where the communication is intercepted. Under the amended definition, "electronic surveillance" would mean: "(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States." In addition to enhancing our intelligence capabilities, this change would advance the privacy rights of Americans, as it would focus the resources of the FISC and the Government on

the review of applications to conduct surveillance that most directly implicate the privacy interests of persons in the United States. This would restore FISA to its original focus and would do so in a way that no longer depends on unforeseeable technological changes.

Additionally, section 401 strikes FISA's current definition of "wire communication". Reference to this term is unnecessary under the new technologically neutral definition of "electronic surveillance".

Section 401 also amends the definition of the term "minimization procedures." This amendment is intended to conform the definition to changes to be made to subsection 102(a) of FISA.

Additionally, section 401 amends the definition of the term "contents" to make that definition consistent with the definition of the same term in Title III (18 U.S.C. 2510), which pertains to interception of communications in criminal investigations. This change would address an inconsistency between subchapter III of FISA (pertaining to pen registers and trap and trace devices) and subchapter I of FISA (pertaining to electronic surveillance). Currently, the definitions of the terms "pen register" and "trap and trace device" in subchapter III of FISA incorporate the definitions provided in 18 U.S.C. 3127. Those definitions, in turn, use the term "contents," which is defined under Title III (18 U.S.C. 2510) to include "any information concerning the substance, purport, or meaning" of a communication. Section 401 would apply this definition of "contents," which Congress already has incorporated into subchapter III of FISA, to the rest of the statute. This change would therefore remove ambiguity from the current definitions.

*Sec. 402. Attorney General Authorization for Electronic Surveillance.*

Section 402 amends section 102 of FISA (50 U.S.C. 1802).

With regard to foreign intelligence targets located within the United States, section 402 alters the circumstances in which the Attorney General can exercise his authority to authorize electronic surveillance without a court order under section 102 of FISA. Currently, subsection 102(a) allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is “solely directed” at the acquisition of the contents of communications “transmitted by means of communications used exclusively” between or among certain types of traditional foreign powers. Changes in communications technology and practices have seriously eroded the usefulness of the current version.

Importantly, this amendment does not change the types of "foreign powers" to which this authority applies nor does it change the handling of incidental information concerning U.S. persons. Any communications involving U.S. persons that are intercepted will be handled in accordance with minimization procedures that are equivalent to those that govern Court-ordered collection.

Section 402 also adds new procedures (section 102A) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. An acquisition under new section 102A must involve obtaining foreign intelligence information from or with the assistance of a communications provider, custodian, or other person who has access to such communications. Appropriate minimization procedures also must be followed.

Finally, Section 402 provides the means through which the Attorney General can compel cooperation with authorizations made under the amended 102(a) or 102A as well as procedures governing the use of information gathered pursuant to section 102A. These are found in section 102B and 102C, respectively. Presently, the Attorney General is authorized to direct a communications

carrier to assist the government with the exercise of electronic surveillance authorized under section 102(a). However, FISA does not currently provide a means by which the Attorney General can seek court assistance to compel compliance with a directive or for recipients of such directives to challenge them in court. The new procedures remedy these deficiencies.

*Sec. 403. Jurisdiction of FISA Court.*

Section 403 amends section 103 of FISA (50 U.S.C. 1803).

Subsection 403(a) amends section 103(a) to provide that judges on the FISC shall be drawn from “at least seven” of the United States judicial circuits, rather than the current requirement that judges be drawn from seven of the circuits.

Subsection 403(b) moves (with minor amendments) a provision that currently appears in section 102 to the section that pertains to the jurisdiction of the FISC.

*Sec. 404. Applications for Court Orders.*

The current procedure for applying to the FISC for a surveillance order under section 104 of FISA (50 U.S.C. 1804) should be streamlined. Currently, the government has to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. Section 404 streamlines the FISA application process to increase the efficiency of the process while still providing the FISC the information it needs in considering whether to authorize the surveillance. For example, subsection 404(1) amends the current FISA provisions requiring that the application contain a "detailed description of the nature of the information sought," and allows the government to submit a summary description of such information. Subsection 404(1) similarly amends the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead permits the government to provide a summary of those facts.

Section 404 also would allow FISA certifications to be made by individuals specifically designated by the President. This change would help resolve a current bottleneck in the FISA process caused by the fact that few officials currently can certify FISA applications. In view of the requirement of a presidential designation, civil liberties still would be protected.

*Sec. 405. Issuance of an Order.*

Section 405 amends the procedures for the issuance of an order under section 105 of FISA (50 U.S.C. 1805) to conform with the changes to the application requirements that would be effected by changes to section 104. It also would extend the initial term of authorization for electronic surveillance of a non-U.S. person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-U.S. persons thereby allowing more resources to be devoted to cases involving U.S. persons.

Additionally, subsection 405(6) amends the procedures for the emergency authorization of electronic surveillance without a court order, to allow the Executive Branch seven days to obtain court approval after surveillance is initially authorized by the Attorney General. (The current period is 72 hours.) This change will help ensure that the Executive Branch has sufficient time in an emergency situation to prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. Subsection 405(6) also would allow for the retention of information if it "contains significant foreign intelligence information."

Subsection 405(8) also adds a new paragraph that requires the FISC, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if requested by the government. This change merely saves paperwork, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard.

*Sec. 406. Use of Information.*

Section 406 amends subsection 106(i) of FISA (50 U.S.C. 1806(i)) which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that unintentionally acquired radio communications between persons located in the United States be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology neutral – the same rule should apply no matter how the communication is transmitted. It would also allow for the retention of information if it "contains significant foreign intelligence information." This ensures that the government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 406 also clarifies that FISA does not preclude the government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information.

*Sec. 407. Weapons of Mass Destruction.*

Section 407 amends sections 101, 106, and 305 of FISA (50 U.S.C. 1801, 1806, 1825) to address weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons.

Subsection 407(a) amends section 101 of FISA to include a definition of the term “weapon of mass destruction.” Subsection 407(a) also amends the section 101 definitions of “foreign power” and “agent of a foreign power” to include groups and individuals engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.”

Subsection 407(b) also amends sections 106 and 305 of FISA to cover the use of information regarding international proliferation of weapons of mass destruction.

*Sec. 408. Liability Defense.*

Telecommunications providers who are alleged to have assisted the government with intelligence activities after September 11th have faced numerous lawsuits as a result of their alleged activities in support of the government's efforts to prevent another terrorist attack. Companies that cooperate with the Government in the war on terror deserve our appreciation and protection – not litigation. This provision would protect providers from liability based upon allegations that they assisted the government in connection with alleged classified communications intelligence activities intended to protect the United States from a terrorist attack since September 11, 2001. Section 408 also provides for the removal of any such actions from state to federal court.

*Sec. 409. Amendments for Physical Searches.*

Section 409 amends section 303 of FISA (50 U.S.C. 1823) to streamline the application process for physical searches, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes parallel those proposed to the electronic surveillance application process.

*Sec. 410. Amendments for Emergency Pen Registers and Trap and Trace Devices.*

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

*Sec. 411. Mandatory Transfer for Review.*

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

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

Additionally, section 411 provides that all litigation privileges are preserved in the originating court, the FISC, the FISA Court of Review, and the Supreme Court of the United States, in any case transferred under that section.

*Sec. 412. Technical and Conforming Amendments.*

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

*Sec. 413. Effective Date.*

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

*Sec. 414. Construction; Severability.*

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