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

November 30, 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-2007-00080

Dear Ms. Hofmann:

This is an interim response to your 31 August 2007 letter to the Office of the Director of National Intelligence, wherein you requested under the Freedom of Information Act (FOIA):

> **". . . 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 34 documents, totaling approximately 250 pages, that have been found to be responsive to your request. Upon review, it has been determined that portions of twelve pages should be withheld on the basis of FOIA Exemption 2, 5 U.S.C. § 552(b)(2). ODNI will continue to review other responsive records and provide a final response to this request as soon as possible.

Sincerely,

John F. Hackett
Director, Information Management Office

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

APR 27 2007

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

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman and Vice Chairman Bond:

I am pleased to provide you with the Administration's proposed fiscal year 2008 Intelligence Authorization Act. Since the creation of the Office of the Director of National Intelligence (ODNI), the Intelligence Community (IC) has embraced and is implementing many reforms, resulting in improvements to important aspects of the IC. The IC has identified additional legislation required to support continuing improvements to intelligence operations. Titles I, II, and III of this proposal are aimed at taking the next steps forward by increasing efficiency and improving the management of the IC. Title IV of our proposed legislation, which I transmitted to you by letter dated April 12, 2007, seeks to address issues with respect to the Foreign Intelligence Surveillance Act (FISA).

The provisions contained in Titles I, II, and III encourage IC integration and promote management best practices. For example, we are requesting the removal of civilian end-strength ceilings. This measure is not aimed at increasing bureaucracy. Instead, the removal of end-strength ceilings is intended to provide the IC with needed flexibility to facilitate implementation of a broad joint duty program. We are seeking to create a new "culture of collaboration" in the IC by integrating the workforce through the use of these joint duty assignments. End strength ceilings place limits on this program. Moreover, the change will permit IC management to ensure that there is an appropriate mix of government employees and contractors. Congressional oversight of the IC workforce is assured by a requirement for an annual projection of employment levels based on mission requirements. The proposal also contains additional human capital provisions to enable implementation of reforms mandated by the Intelligence Reform and Terrorism Prevention Act of 2004.

Similarly, the IC must continue to improve information sharing and move from a "need to know" to a "responsibility to provide" culture. Our proposal, therefore, seeks to adjust 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 initial two-year period. We are also requesting authority to use National Intelligence Program (NIP) funds to quickly address deficiencies and immediate requirements that arise throughout the course of intelligence production and information sharing.

To protect against the threats facing this country, the American people deserve the most effective intelligence apparatus possible. Over the past two years, the IC has achieved positive results through a concerted effort to integrate itself more tightly, manage its resources more strategically, and share information more freely. However, there is more left to do and I urge you to enact these important proposals.

The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presenting of these legislative proposals for your consideration and the consideration of Congress at this time. As I continue to work to transform the IC, I may transmit additional proposals for your review. My staff and I look forward to working with the Congress to continue the process of reform and ensure the enactment of this important legislation. If you have additional questions, please contact me or my Director of Legislative Affairs, Kathleen Turner, on [redacted]

Sincerely,

J. M. McConnell

Enclosure

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

September 26, 2007

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

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

The Honorable Ron Wyden
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman, Vice Chairman Bond, and Senator Wyden:

(U//~~FOUO~~) During the September 20, 2007 closed Hearing before your committee on the Foreign Intelligence Surveillance Act and the Protect America Act, Senator Wyden asked the DNI to respond in writing to the following question:

> "Under the Protect America Act, if the US 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 US 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?"

Attached please find our response to that question. We have also enclosed a detailed explanation of NSA's Minimization Process and Procedures in both classified and unclassified form.

(U) If you require additional information, please contact me at [redacted]

Sincerely,

Kathleen Turner

Kathleen Turner
Director of Legislative Affairs

Enclosures: As stated.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

July 26, 2007

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

Dear Chairman Reyes:

(U) On July 25, 2007, Director of National Intelligence (DNI) Mike McConnell wrote you regarding the urgent need to modernize the Foreign Intelligence Surveillance Act (FISA). Attached please find the classified attachment the DNI referred to in his letter.

(U) If you require additional information, please contact me at [redacted]

Sincerely,

Kathleen Turner

Kathleen Turner
Director of Legislative Affairs

Enclosure: As stated.

cc: Members of the HPSCI

UNCLASSIFIED WHEN SEPARATED FROM ENCLSOURE

~~TOP SECRET//SI//NF//MR~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

July 26, 2007

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

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

The Honorable Carl Levin
Select Committee on Intelligence (Ex-Officio)
United States Senate
Washington, DC 20510

Dear Senators:

(U) On July 24, 2007, Director of National Intelligence (DNI) Mike McConnell wrote you regarding the urgent need to modernize the Foreign Intelligence Surveillance Act (FISA). Attached please find the classified attachment the DNI referred to in his letter.

(U) If you require additional information, please contact me at [redacted]

Sincerely,

Kathleen Turner
Director of Legislative Affairs

Enclosure: As stated.

cc: The Honorable Christopher S. Bond
The Honorable Arlen Specter
The Honorable John McCain

UNCLASSIFIED WHEN SEPARATED FROM ENCLSOURE

~~TOP SECRET//SI//NF//MR~~

Senate Committee on the Judiciary

Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act

25 September 2007

Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

STATEMENT FOR THE RECORD OF
J.MICHAEL McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
JUDICIARY COMMITTEE
UNITED STATES SENATE

September 25, 2007

Good morning Chairman Leahy, Ranking Member Specter, and Members of the Committee:

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and am sensitive to the fact, that FISA and the Protect America Act and the types of activities these laws govern, are of significant interest to Congress and to the public. For that reason, I will be as open as I can, but such discussion comes with degrees of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities. Therefore, on certain specific issues, I am happy to discuss matters further with Members in a classified setting.

I have not appeared before this Committee previously as a witness, and so I would like to take a moment to introduce myself to you. I am a career intelligence professional. I spent the majority of my career as a Naval Intelligence Officer. During the periods of Desert Shield and Desert Storm, as well as during the dissolution of the Soviet Union, I served as the primary

Intelligence Officer for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense. I then had the privilege of serving as the Director of the National Security Agency (NSA) from 1992 to 1996, under President Clinton. In 1996, I retired from the U.S. Navy after 29 years of service - 26 of those years spent as a career Intelligence Officer. I then turned to the private sector as a consultant, where for ten years I worked to help the government achieve better results on a number of matters, including those concerning intelligence and national security. I have been in my current capacity as the nation's second Director of National Intelligence (DNI) since February 2007.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, 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 or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before this Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new,

the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence

Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain

what I mean by that. 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 international 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.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain "in wire" or fiber optic cable transmissions fell 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."

Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed 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.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they

needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and

mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. 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, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of

foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and
- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

Common Misperceptions About the Protect America Act

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in

order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only "foreign-to-foreign" communications from FISA's scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the

IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is who the target is, and where the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

(a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to the House and Senate Intelligence Committees regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of this Committee and the Judiciary Committee of the House of Representatives, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of the House Permanent Select Committee on Intelligence requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a

site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed House Intelligence Committee staff members regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four House Intelligence Committee staff members for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from the House Intelligence Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from the Senate Intelligence Committee and two staff members from this Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ's National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from the House Intelligence Committee, and the Senate Intelligence, Armed Services Committees, and this Committee regarding the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on the House Intelligence Committee and four of that Committee's staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four House Intelligence Committee staff members and the Committee's Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House Judiciary Committee staff member. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

On September 17, 2007, representatives from the ODNI and the Department of Justice provided briefings regarding implementation to staff members from the House Judiciary Committee.

On September 18, 2007, Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division, my General Counsel, Ben Powell, and I testified before the Judiciary Committee of the House of Representatives on the Protect America Act.

On September 19, 2007, representatives from the ODNI and the Department of Justice provided briefings regarding implementation to staff members from this Committee.

On September 20, 2007, Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division and I testified before the House Permanent Select Committee on Intelligence in regard to the Protect America Act.

Also on September 20, 2007, I was joined by National Security Agency Director (NSA), Lieutenant General Keith Alexander; Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division; Acting Assistant Attorney General from the Department of Justice's Office of Legal policy, Brett Gerry; Federal Bureau of Investigation (FBI) Deputy Director John Pistole and the General Counsels

of the ODNI, FBI, and NSA to speak to a closed session of the Select Committee on Intelligence of the Senate on the Protect America Act.

Additional Member and staff briefings shall follow.

Lasting FISA Modernization

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

Making the Changes Made by the Protect America Act Permanent

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed,

however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will 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. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

August 29, 2007

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

Dear Director McConnell:

I am writing to seek clarification on representations that you made to me and other members of Congress during our discussions on passing a temporary Foreign Intelligence Surveillance Act (FISA) fix that could garner strong bipartisan support prior to the August congressional recess.

Allow me to be direct and to the point: at a critical juncture in our negotiations, you gave assurances that were not fulfilled, and made agreements that were not kept. No explanation has ever been provided to me then or since as to why you to did not carry out these commitments. As a result, I and others involved in these important and intense FISA negotiations are left to question whether the negotiations were carried out in good faith or whether your commitments were overruled by others at the White House or within the Administration.

The net result is that a realistic opportunity to pass the stop-gap authorities the Intelligence Community needed with overwhelming bipartisan support was lost. Until these discrepancies are resolved, a dark cloud will continue to linger over the events preceding the Senate votes of Friday, August 3rd. Looking ahead, as the Committee plans to consider a more lasting FISA bill, I need to be assured that there will not be a repeat of the past. Too much is at stake for our collective efforts to be undercut by doubt and suspicion.

I do not raise this matter lightly. But each of us must have confidence in what the other one says and commits to, especially on matters of national security. I know that you are strongly committed to carrying out your duties as Director of National Intelligence. I have been a vocal supporter of yours and have publicly lauded your qualifications to lead the Intelligence Community. And I share your view that FISA needs to be reformed and brought up to date.

As you know, I along with Vice Chairman Bond wrote to you and others in the Administration on March 23rd of this year requesting a FISA bill and the Committee held numerous hearings on the proposed legislation with the hope of passing modernization legislation before we adjourned for the year. I even agreed to hold these hearings despite the Administration's continued stonewalling in providing the Committee long-overdue documents critical to our understanding and oversight of the President's warrantless surveillance program. In late June, I personally called the Vice President offering a compromise agreement to break the impasse over documents and access so that we could proceed to an expeditious markup FISA and carrier liability legislation.

In order that we may move forward on FISA legislation in a constructive and collaborative manner, it is important that I receive from you a detailed and responsive explanation to the discrepancies contained in the following chronology:

On Thursday, August 2nd, at approximately 12:00 noon, my staff sent your staff a revised FISA bill reflecting DNI input to the July 31st version of my proposed bill. Later that day, at about 2:00 pm, you and I spoke by phone to discuss the bill. I asked you directly what specific changes to the bill would have to be made in order to make the bill acceptable, if not ideal, to you and a bill that you could publicly endorse. You responded by saying that three changes were required before you could endorse the proposal: (1) clarity that no individualized court warrants are required for foreign targeting; (2) drop the "terrorism" limitation on the foreign intelligence collection authority; and (3) eliminate the provision that would require the Attorney General to submit to the Foreign Intelligence Surveillance Court (FISC) his guidelines for when "significant contacts" between a targeted foreigner and a U.S. person would necessitate an individualized court warrant against the U.S. person. You described this third issue as a "poison pill."

During our conversation, you said you would, using my latest FISA bill proposal as a baseline, send back to me a revised version of the bill making these three changes and, furthermore, that you would agree to the six month sunset included in the bill. You also agreed to the point I made during our conversation that it was essential for you to publicly endorse the agreement as sufficient in giving the Intelligence Community the interim authorities needed, even if it is not your entirely preferred legislative formulation, in order for the bill to pass on the Senate floor with broad support.

House Intelligence Committee Chairman Reyes informed me that you had an almost identical conversation with him just before and after our call in which you listed the three changes needed to gain your endorsement.

Later in the day, at approximately 5:30 pm, a meeting was convened in Speaker Pelosi's office attended by the Speaker, House Majority Leader Hoyer, Chairman Reyes, Senate Majority Leader Reid, Senator Levin and myself. In a speaker phone call with the members, you reiterated the same points made earlier in separate phone calls to me and Chairman Reyes and that with these limited changes you would agree to support the revised bill along with a six month sunset provision.

During this conversation, you also assured the assembled members that you were independent of the White House's direction on this matter and that you were authorized to negotiate the deal you felt would give the Intelligence Community the required authorities to address collection shortfalls while a more lasting bill was crafted and passed into law.

You stated in the conversation that you realized that the collection order must come from the FISC and not the Attorney General, a concession you were making to the reality that the companies may not promptly cooperate without a court order given concerns over pending litigation.

You also told members that if they dropped the "significant contacts" guidelines provision your concern that the FISC may feel it is obligated to issue individualized warrants rather than a one-time order based on the reasonableness of the guidelines for determining targets are foreign would go away. In other words, your three needed changes were actually two.

You specifically stated to the members that you could agree to the latest congressional FISA bill offer if the "terrorism" only limitation and the provision requiring that the "significant contacts" guidelines be part of the submission to the FISC were removed.

All of the assembled members agreed to accept these changes and felt they reached an agreement with you on the scope and content of the FISA bill. You told members that you would need 30 minutes or so for your staff to make these two changes and again agreed to use the latest congressional offer as the baseline document.

In response to separate remarks made by Leader Hoyer, Chairman Reyes, and me, you stated that you could publicly endorse the bill as modified, and in response to the question from Leader Hoyer you said that the modified bill would be a "7" on a scale of 1-10, with "10" representing ideal.

After a half-hour passed without receiving either the revision to the bill text or a call from you, the assembled members called you and were told that you were on the phone with the White House. When you returned their call, in the vicinity of 7:00 pm, you stated that you were "under enormous pressure from the other side" not to negotiate any concessions from your latest offer. You assured members that you would hold firm however, but that you needed additional time to work on the language that would be passed back to members.

The revised bill forwarded by your office later in the evening of August 2nd was not what you promised to members. Specifically:

- the bill passed back to members used the earlier DNI bill as the baseline for changes, not the most recent congressional proposal as promised;
- the bill did not include a six month sunset provision as promised;
- the bill allowed for a lengthy emergency collection prior to the Attorney General's submission to the FISC of his foreign targeting guidelines (for 90 days vice the 15 days included in the congressional bill) and allowed the collection to continue ostensibly for the entire six months contemplated while a denial of the court was under appeal;
- the bill dropped the requirement on the Attorney General to have any guidelines on "significant contacts" between foreign targets and U.S. persons;
- the bill dropped the Inspector General review provision;
- the bill changed the definition of "electronic surveillance in the FISA; and
- the bill included a number of other language changes of concern to members.

I and other members were left with deflating realization that either the negotiations were not carried out in good faith or that the agreement you had reached with congressional leaders a mere three hours earlier had been overturned by pressure from the White House and/or others.

- Why did the bill you sent back on the evening of August 2nd not comport with what you promised members by phone?

- Why did the bill not use the most recent congressional proposal as a baseline for the two agreed-to changes as you promised?

- Why did the bill include other changes beyond the scope of those discussed with members?

- Why did the bill not include a six month sunset provision as you promised?

- To what extent did you submit the agreement you reached with the members to the White House, other Administration officials, and Republican members of Congress for their concurrence?

- In what respect was the agreement you reached with the members altered or overruled by these subsequent discussions?

- Why did you or a senior member of your staff not contact the members with whom you reached the agreement and provide them with an explanation as to why the bill sent back was not what was promised three hours earlier? To the best of my knowledge, none of the members who participated in the discussions were called by you or a member of your staff on August 2nd, or since then, with an explanation for these discrepancies.

The next morning, Friday, August 3rd, I joined with Senator Levin and others to take the bill you sent the evening before and make the changes, such as adding the six month sunset provision, that we believed were agreed to the previous evening. Our hope was to use the bill you provided and modify it in a way that was consistent with our discussions with you and that could garner broad bipartisan support.

An agreement was reached between the Senate leaders on Friday to hold separate votes on the (Senator) McConnell-Bond FISA bill and the Rockefeller-Levin FISA bill. The McConnell-Bond bill had been filed on August 1st and was not the proposal you forwarded on the evening of August 2nd. And, to reiterate, the Rockefeller-Levin bill was your August 2nd bill, modified to incorporate the tenets of the agreement reached but not carried out less than 24 hours before.

At 4:39 pm on Friday, *your office issued a public statement* urging that the Senate support the legislation you provided the night before; in other words, *your* August 2nd bill, not the August 1st McConnell-Bond bill.

Later that evening, you arrived off the Senate floor during the debate of the two bills and you issued a second statement, amending your 4:39 statement, saying that you could not support the Rockefeller-Levin modified DNI bill and urging Senators to support the bill sponsored by Senators McConnell and Bond.

- Why did your statements of August 3rd change from initially calling on members to support your August 2nd bill to then calling on members to support the August 1st bill sponsored by Senators McConnell and Bond?

- In what specific respects was the Rockefeller-Levin modified DNI bill inconsistent with the agreement you reached with members by phone on August 2nd?

- In what specific ways was the Rockefeller-Levin modified DNI bill unacceptable to you?

- Were you requested or directed by any official to publicly urge the defeat of the Rockefeller-Levin modified DNI bill? If so, by whom?

We both share a common goal of improving our intelligence capabilities in ways that will strengthen our Nation's security. Achieving this goal requires close cooperation between the executive and legislative branches of government that is built upon trust. We can ill-afford an environment where commitments made are not kept. I look forward to your response to the questions I've posed in a timely fashion so that we can clear the air and move on in a constructive manner.

Sincerely,

John D. Rockefeller IV
Chairman

United States Senate
Select Committee on Intelligence

Fax

To: Director McConnell

Fax Number: [redacted] Phone Number: _____

From: Senator Rockefeller

Date: 8/30/07

Number of Pages: 7 (Including Cover Page)

Comments: _____

Please Contact Sender if this fax is not complete. (202) 224-1700

SHELDON WHITEHOUSE
RHODE ISLAND

COMMITTEES
AGING
BUDGET
ENVIRONMENT AND PUBLIC WORKS
INTELLIGENCE
JUDICIARY

United States Senate
WASHINGTON, DC 20510-3905

https://whitehouse.senate.gov
(202) 224-2921
TTY (202) 224-7746

170 Westminster Street, Suite 1100
Providence, RI 02903
(401) 453-5294

RECEIVED
18 Sep 07

September 4, 2007

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

Dear Admiral McConnell:

While I look forward to continuing to work with you, I wish to convey to you: one, my deeply felt displeasure with the administration's legislative strategy on the recent "FISA Fix"; two, my belief that the people we serve were ill-served by it; and three, my concern that as a result we passed contentious and second-rate legislation rather than a well-considered, first-quality product which had earned the consensus that legislation of this nature deserves. As you may know, I was prepared to work arduously to achieve such a result, and put enormous effort into the unsuccessful attempt to achieve that result in the final week.

My concerns are perhaps best illustrated by the following timeline. On July 11, we met in the secure confines of the SSCI regarding your request to expedite certain changes you wished in your legal authority. In that very meeting, I told you I was on board, but would need to see your actual proposed legislation as soon as possible since on these things the specific language is key, and "the devil is always in the details." The letter that accompanied your initial draft legislation was dated July 27, a Friday, 16 days later. I first received the draft legislation on Monday, July 30. That gave two bodies of Congress with 535 total members five days to review, edit and approve the expedited legislation you had taken 16 days to draft.

The initial bill taken from the draft was rushed to the floor on Wednesday, August 1, with little review and great haste. It is not clear that its sponsors had even read it carefully.

It appears that the bill was slow-walked in your shop for 16 days – during which period the urgency expressed in the final week on the Senate floor, and by you in press releases, would presumably have been as real as it was in the final week. Yet with all the urgency of threatened immediate mass casualty attacks being planned, with all the resources of the DNI, the Pentagon and the White House behind you, somehow it took 16 days to write 12 pages of draft legislation. This resulted in the bill not being filed until Wednesday of the last week of session, timed with a volley of those panicky floor speeches, and Presidential media events, to create the atmosphere of a stampede.

The stampede worked. You won. But you did so at a substantial price, one that will be paid in rancor, suspicion and distrust, and one that reflects a long step backward on the path away from the divisive partisanship that impeded oversight and impaired this Committee for so many years. The costs are real when we fail, as demonstrated by the incalculable loss in the disaster presently unfolding in Iraq.

The manner in which this episode was handled was in my view disrespectful of this institution I serve, disrespectful of the common purpose our patriotism binds us to achieve, and disrespectful of the principle I hold dear in politics that honorable good will produces better results over time than calculated manipulation. We slow ourselves down a lot, and we limit our collective options considerably, if we create an atmosphere in which every horse has to be examined for its Trojan compartment, and every venture assayed for its twisted motivation.

In the long run, we will serve America better if we work in an atmosphere of cooperation and trust.

Respectfully yours,

Sheldon Whitehouse
United States Senate

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 20 2007

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

Dear Mr. Chairman:

Thank you for your letter of August 29th 2007, regarding the "Protect America Act of 2007" (Pub. L. No. 110-055, 121 Stat. 522) and the alternative Rockefeller-Levin approach (S.2011). I want to thank you for the time and effort you and other Members of Congress spent working to close the gaps in our intelligence capability prior to the August recess. Those of us responsible for implementation of the Protect America Act (PAA) also appreciate the need for regular and meaningful reporting to Congress. As outlined in the attached Department of Justice letter of September 5th 2007, and the letter of September 17th 2007 from the Civil Liberties and Privacy Officer of the Office of the Director of National Intelligence of September 18th 2007, use of this authority will be subject to rigorous oversight. Our goal is to provide transparency, so that Congress may evaluate our implementation of the new authorities effectively.

In your letter you asked me whether I was directed to publicly urge the defeat of S. 2011. My answer is an unequivocal no. Upon my arrival as Director of National Intelligence, I learned that our collection using the authorities provided by the Foreign Intelligence Surveillance Act (FISA) were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information. I turned to my colleagues in the Intelligence Community (IC) to ask what could we do to repair this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. Building upon their work, I made fixing FISA a priority. At all times the Administration relied on me to use my professional judgment on how to do so. As the head of the nation's IC, it is 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.

As you note, we share the common goal of improving our intelligence capabilities. Throughout my discussions with Congress, I articulated certain principles that were necessary to achieve this goal. Foremost among them was the view that FISA should be modernized to remove targets outside the United States from those activities requiring FISA Court approval, while continuing the FISA requirement that the government obtain an order authorizing electronic surveillance if the target of the foreign intelligence surveillance is a person reasonably believed to be in the United States.

Your letter posed a number of questions about pressure allegedly exerted on me and raised questions about the course of the negotiations. First, statements issued by my office

reflected my best professional judgment. Second, there were many conversations where general concepts were discussed. However, as everyone in this process recognized, FISA is an extremely complex statute and small changes can have significant operational impacts. We could not agree to unseen bill text that may result in unanticipated consequences. In addition, we did modify proposals provided to us in order to ensure we could accomplish our mission.

Your letter discusses a number of specifics about discussions on August 2nd concerning various FISA proposals. Our efforts on August 2nd were directed toward reaching agreement on a bill that reflected the principles we discussed and was technically correct in order to allow the IC to move forward with clarity and speed to close critical gaps. In addition to the major issues raised by the draft provided us on August 2nd, such as the limitation of collection to "international terrorism," the proposal provided to us on August 2nd contained a number of technical requirements that raised concern among intelligence professionals.

For example, the proposal mandated that FISA applications contain a number of details, including specifying the "foreign power" and the "nature of the information sought," that – without further clarity – have proved to be quite significant requirements based on past experience. The emergency authorization provision appeared to only be in effect for "15 days following enactment," and therefore appeared to provide no emergency authorization authority if we encountered an emergency situation that occurred after this period. The Inspector General review provision appeared to require the provision of data that is not technically available and did not appear to provide for a role for those Inspector Generals' offices most directly responsible for oversight of Signals Intelligence activities.

Thus, the proposal we provided to you on the evening of August 2nd reflected these concerns, while trying to incorporate as much of the proposal your staff provided to us as possible. All of this was done under extreme time pressure. We certainly did not think that providing changes to these provisions was done in bad faith, but instead reflected our considerable concern about the impact of these provisions. While my discussions with members of Congress concentrated on high-level principles, and were not detailed discussions of unseen bill text in many cases, given the complexity of the statute in question, and the operational importance of the issue to our national security, I always expected that experts in this area would need to examine each line of any proposal for its impact on our operations.

Perhaps our discussions could have been more clear in terms of the fact that there were additional technical parts of the proposals that raised concerns beyond the general principles we discussed. I regret any misunderstanding on this point, but at all times we sought in good faith to incorporate the principles we discussed while revising technical issues raised in various drafts.

We also believe it is critical to note the extreme time pressure and deadlines placed on our staffs. We were extremely concerned about passage of a proposal that lacked clarity or had significant unintended consequences in terms of damaging ongoing intelligence efforts. Much of these unfortunate misunderstandings may in fact arise from the short deadlines to draft proposals in a complex area.

Your letter also raises a number of questions concerning S. 2011, the Rockefeller-Levin bill introduced on August 3rd. We recently provided a letter outlining our concerns with S. 2011 and a copy is enclosed.

Finally, we believe we acted in good faith throughout this process as did all the members of Congress who devoted extraordinary time and effort on a bipartisan basis to ensure we did everything possible to close critical gaps in our capabilities. I can assure you that my actions reflected one thing – and one thing alone: My best professional judgment as to what was required by the Intelligence Community to protect the country while ensuring the continued protection of the civil liberties of all Americans.

Thank you again for this opportunity to comment and for your thoughtful consideration of proposals to fix critical gaps in our intelligence operations. I look forward to continuing our dialogue and working with you further on this important issue.

Sincerely,

J.M. McConnell

Attachments: as stated

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

SEP 2 0 2007

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your letter of August 7, 2007, regarding the "Protect America Act of 2007" (Pub. L. No. 110-055, 121 Stat. 522) and the alternative Rockefeller-Levin approach (S.2011). We appreciate the time and effort you and other Members of Congress spent working to close the gaps in our intelligence capability prior to the August recess. We are also grateful for this opportunity to clarify issues related to the Protect America Act (PAA), as we work to achieve permanent Foreign Intelligence Surveillance Act (FISA) modernization.

Please know that those of us responsible for PAA implementation appreciate the need for regular and meaningful reporting to Congress. As outlined in the Department of Justice letter of September 5, 2007, use of this authority will be subject to rigorous oversight. Our goal is to provide transparency, so that Congress may evaluate our implementation of the new authorities effectively.

As I stated on the evening of August 3, 2007, by incorporating new and undefined terms S.2011 "creates significant uncertainty in an area where certainty is paramount to protect the country." We received the final text of S. 2011 as the Senate was beginning its debate on the night of August 3. In the short time given, we opted to support the bill that we believed would give the Intelligence Community (IC) the best chance to close the gap in our intelligence coverage with the least amount of ambiguity. It is unfortunate that there has been misunderstanding regarding the decision. However, for the reasons stated below, we believe that our decision was correct and under the PAA the IC has effectively closed critical gaps.

Let us assure you that it was not our intent to suggest that U.S. persons outside the United States be subject to surveillance to the same extent as non-U.S. persons outside the United States. We understand that there may be some concern because section 105A of the PAA does not appear to make this explicit distinction. Our April proposal did not alter the approach to U.S. persons abroad nor did it modify the protections provided by Section 2.5 of Executive Order 12333. Similarly, under the PAA, the IC will continue to apply Section 2.5 of Executive Order 12333, adopted in 1981, and as has been the standard practice of the IC since 1978.[1]

[1] A similar provision was contained in section 2-2(b) of Executive Order 12036, the predecessor of Executive Order 12333.

S. 2011 contained a number of modifications to the proposals we submitted to the Congress. We were concerned about the impact of a number of these modifications. This uncertainty, in the short time available, led us to conclude that the only viable decision we could make was to support the bill that we knew gave the IC clear authority to close intelligence gaps.

First, S. 2011, unlike the proposal we submitted, stated that a FISA application was not required to identify "the persons, other than a foreign power," against whom the electronic surveillance will be directed. This could have reasonably been interpreted to require that analysts make a foreign power connection for an overseas target prior to filing an application. We do not believe that this is an appropriate request for targets located overseas. It is unclear what purpose this requirement would serve in the case of a foreign terrorist or weapons proliferator overseas, whose connection to an identified foreign power may be unclear, other than to provide privacy protections to the person located overseas. As we stated while Congress was considering proposals to amend FISA, the IC should be able to collect against valid foreign intelligence targets. Moreover, Section 407 of our April proposal noted that the current definition of "foreign power" contained in FISA is not sufficient and requested that the definition be expanded to include a group engaged in "the international proliferation of weapons of mass destruction."

Second, S. 2011 added a new section requiring the issuance of certain new Attorney General guidelines related to U.S. persons within 15 days of enactment. We understand that this concern relates to the issue commonly referred to as "reverse targeting." Throughout our discussions with Congress, we have stated that the government should be required to obtain an order authorizing surveillance if the target of foreign intelligence surveillance is a person reasonably believed to be in the United States. Moreover, FISA – both before enactment of the PAA and after – requires that if the target is in the United States, the IC must seek FISA Court authorization to conduct in order to undertake such electronic surveillance. Consequently, we believe that a reverse targeting provision in the law is unnecessary because it is already unlawful for the IC to engage in reverse targeting. Additionally, the National Security Agency (NSA) has longstanding minimization procedures to address the handling of incidentally acquired U.S. person information. However, because of these concerns, this is an area that my Civil Liberties Protection Officer and General Counsel, together with the Department of Justice, are working closely with NSA and other IC elements on implementing the PAA, to review.

The new subsection 105B (d) (2) in S. 2011 appeared to potentially rewrite the minimization framework that has worked well for decades. This subsection requires that guidelines be designed to ensure that an application for a FISA Court order, under section 104, is made when electronic surveillance "is of a nature or quantity as to infringe on the reasonable expectation of privacy of persons within the United States." We all, of course, share the goal of ensuring that our activities do not violate the legal rights of persons within the United States. In particular, NSA's activities, including its minimization procedures, have been carefully calibrated and implemented to provide a consistent and effective mechanism to ensure the constitutional reasonableness of its surveillance activities. The new subsection 105B (d) (2) in S. 2011 appeared to create ambiguity as to the legal sufficiency of the current procedures and the large processing and training infrastructure that are based on them. As these are complex issues, we were concerned that it would take months to determine the legal impact of the new provision

on the traditional legal analysis upholding the existing procedures, to craft new guidelines as needed, and even longer to retrain the workforce on the new guidelines. In the limited time we were given, no intelligence professional who reviewed the proposal could assure us as to the content – or the long-term consistency and clarity -- of new Attorney General guidelines governing the "nature or quantity" of a potential "infringement" on an expectation of privacy.

Third, we were concerned about ambiguity in the wording of the proposed Section 105B (b) (1) (B) (iii). This provision provides that the DNI and Attorney General must certify that "to the extent any acquisition" constitutes electronic surveillance under subparagraph (2) and (4) of section 101(f) of FISA, such acquisition "is approved or minimized as appropriate." Although "minimized" is a reference to the IC's minimization procedures, the meaning of "approved as appropriate" is unclear in this context. Does this mean approved by the Court or by the Attorney General? Similarly, what process constitutes appropriate approval? While we presume the intent of the reference is to the approval process contained in the proposal, the impact on intelligence collection could be significant depending on court interpretation.

Fourth, unlike our proposals that remove the targeting of persons located overseas from FISA's definition of "electronic surveillance," S. 2011 only removed communications "between foreign persons located outside the United States." S. 2011 would keep targeting of persons located overseas for foreign intelligence purposes within the FISA definition of "electronic surveillance" unless we could know in advance with certainty if the communication is "between" persons overseas. This is a very difficult task to determine in advance, and is fundamentally at odds with all proposals we submitted to remove such activity from FISA.

Finally, we should note that because of the critical gaps facing the country – and against the principles we have consistently articulated since April 2007 – we did provide a proposal at congressional request that provided for FISA court approval of foreign intelligence collection from foreign targets overseas. We did not think at the time that this was an appropriate role for the court and was extremely concerned that the approach would hamper our operations without corresponding civil liberties protection benefits. Such a requirement would likely evolve into a situation where significant analyst expertise is diverted on an on-going basis to court filings. As you note, the PAA does provide for FISA Court review of procedures. That was a major concession in order to accommodate the interests of all.

Thank you again for this opportunity to comment and for your thoughtful consideration of proposals to fix critical gaps in our intelligence operations. We look forward to continuing our dialogue and working with you further on this important issue. If you have any questions on this matter, please contact the Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

J. M. McConnell

OFFICE of the Director of National Intelligence
Washington, DC 20511

September 17, 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:

I am writing this letter in response to a request from the Ranking Member of the House Permanent Select Committee on Intelligence. I appreciate this opportunity to describe the civil liberties and privacy protections that my office is charged with overseeing in the implementation of the Protect America Act of 2007.

Role of the Civil Liberties Protection Officer. I am the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). Congress has entrusted me with statutory responsibility to "ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures" of the Intelligence Community. 50 U.S.C. § 403-3d(b)(1). As a result, my office is working closely with the Department of Justice and the DNI's Office of General Counsel, to help ensure that the intelligence agencies that implement the authorities under the Protect America Act have put in place adequate safeguards to protect the privacy and civil liberties of American citizens, legal residents, organizations and corporations ("U.S. persons"), as required by law and by the rules that have traditionally governed our intelligence activities. In addition, my office is working with the Department of Justice and DNI's Office of General Counsel to conduct formal, periodic assessments of compliance by agencies exercising authorities under the Protect America Act, and briefing the staffs of various congressional committees frequently and in depth.

The Larger Context - Protection of Civil Liberties and Privacy in the Intelligence Community. In order to understand the civil liberties and privacy protections that are being implemented under the Protect America Act, it is important to put the Act in the larger context of

how the Intelligence Community has historically protected information about Americans. As you know, intelligence agencies collect, retain, and disseminate information about U.S. persons. One of the limitations placed on the collection and use of U.S. person information is found in Executive Order 12333. That Executive Order provides that collection of intelligence is to be "pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the Constitution was founded." It was signed by President Reagan in 1981, building on similar orders signed by Presidents Ford and Carter, to address the findings of the Church and Pike committee investigations of the mid-1970s. It put in place key restrictions on intelligence activities, sometimes referred to as "U.S. person rules," and has become part of the fabric of the Intelligence Community.

These rules – further detailed by procedures approved by the Attorney General for each agency – are not implemented in a vacuum. They are interpreted and applied by offices of general counsel at each intelligence agency, with compliance audited by offices of inspector general.[1] And of course, as you and the members of your committee are well aware, a critical outcome of the Church and Pike reports was the establishment of the House and Senate Intelligence Committees. Since the nature of intelligence by necessity requires secrecy, and therefore full transparency cannot be provided to the public at large, the Intelligence Committees, by exercising oversight over classified activities, can ensure that the Intelligence Community is protecting the nation from foreign threats while at the same time protecting our civil liberties.[2]

The Protect America Act. As Director McConnell and others have explained, as a result of technology changes in the global communications network, in recent years a substantial volume of communications of persons in foreign countries have been subject to the Foreign Intelligence Surveillance Act (FISA) despite Congress's intent in 1978 to exclude such activities. These changes resulted in applying the framework of probable cause and prior court review to foreign intelligence targets in foreign countries. In passing the Protect America Act, Congress changed the law to exempt from electronic surveillance "surveillance directed at a person reasonably believed to be located outside the United States" in order to obtain "significant foreign intelligence." As a result, probable cause and prior court review are not required for surveillance of foreign intelligence targets in foreign countries for foreign intelligence purposes.

Congress was concerned, however, with (1) whether the target of the surveillance is really in a foreign country, and (2) the privacy and civil liberties interests of U.S. persons who may be in communication with the target. To address these two issues, Congress required the Director of National Intelligence and the Attorney General to certify two separate sets of procedures with respect to acquisitions conducted under the Protect America Act:

---

[1] Violations of these rules are required to be reported to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board. See Executive Order 12334 (Dec. 4, 1981) (establishment of Intelligence Oversight Board).

[2] Moreover, violations of law are required to be reported to the Intelligence Committees. See National Security Act of 1947, as amended, 50 U.S.C. § 413(b).

(1) reasonable procedures for determining that surveillance to be conducted pursuant to the Protect America Act concerns persons reasonably believed to be outside the United States ("foreign targeting procedures"), which must be reviewed by the FISA court, and

(2) minimization procedures that meet the definition of "minimization procedures" under FISA.[3]

In conjunction with the Department of Justice and the DNI's Office of General Counsel, we are focusing our oversight on ensuring that both sets of procedures adequately protect the privacy and civil liberties of U.S. persons, and that they are being followed by agencies of the Intelligence Community.

Is the target really a foreign intelligence target in a foreign country?

My office, the Department of Justice, and the DNI's Office of General Counsel has reviewed the foreign targeting procedures to ensure that they protect privacy and civil liberties, and is involved in reviewing their implementation to ensure that the procedures are followed. The statute does not require perfection, but it does require procedures that ensure collection is only undertaken against persons "reasonably believed to be outside the United States."

The need to perform this analysis is nothing new for the National Security Agency or other Intelligence Community agencies. Agencies have developed, over decades, policies and procedures to ensure that their monitoring activities did not inadvertently collect domestic information by mistake. However, in the Protect America Act, Congress went a step further, by requiring these procedures to be certified by the Director of National Intelligence and the Attorney General and submitted for review by the Foreign Intelligence Surveillance Court.

Significantly, the statute applies the foreign targeting procedures to "the acquisition of foreign intelligence information . . . ." As a result, the Intelligence Community's procedures for this kind of collection must enable analysts to determine, prior to obtaining any communications under the Protect America Act, that there is a reasonable belief that the target is a foreign intelligence target in a foreign country. Detailed procedures, which have already been submitted to the Foreign Intelligence Surveillance Court, explain how this is done. The procedures are classified because they discuss precisely how the Intelligence Community performs collections. However, I can describe them in general terms.

This "foreign targeting" determination that analysts must make may be relatively straightforward for certain forms of communication, and may be more complex for other forms of communication. The Intelligence Community uses a variety of sources of information, including technical analysis, information about the target from other intelligence reporting, and databases that are commercially available or otherwise lawfully obtained. Analysts are generally

[3] Section 105B of FISA, as amended by the Protect America Act, requires the Director of National Intelligence and the Attorney General to certify, among other things, that: "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be outside the United States, and such procedures will be subject to review of the [FISA] Court . . ." and that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under [FISA]."

able to assess, with a high degree of confidence, whether a particular foreign intelligence target is in a foreign country. When they cannot do so, they will not initiate collection against that target.

While the procedures require this foreign targeting determination to be made prior to initiating collection, a variety of means are also employed to verify that the determination continues to be accurate after collection has begun. Even where the initial decision was correct, the location of the target may change. The Intelligence Community does not simply rest on its initial decision. Methods used to double-check the foreign targeting determination are employed frequently, even daily in some cases.

Questions have been raised about Americans traveling or residing abroad. Section 2.5 of Executive Order 12333 protects Americans – and U.S. persons generally – who may be encountered by the Intelligence Community overseas, by prohibiting the use of techniques that would require a warrant if used for law enforcement purposes, unless the Attorney General has determined that there is probable cause to believe the U.S. person is an agent of a foreign power. This requirement – in place since 1981 – has been judicially reviewed and upheld,[4] and is not affected by the Protect America Act. As a result, analysts must – and do – take steps to ensure that their "foreignness" determinations under the Protect America Act not only involve an assessment of the target's location, but also of whether the target may be a U.S. person. If the target is a U.S. person, collection may not be initiated without authorization under section 2.5 of Executive Order 12333, based on a finding of probable cause that the target is an agent of a foreign power.[5]

Questions have also been raised about "reverse targeting" – that is, could an intelligence agency target a person overseas as a pretext for intercepting the communications of the individuals inside the United States with whom the foreign person is in contact? The simple answer is that when the agency's actual purpose is to surveil the person in the United States, it must obtain a court order as required under FISA. This is also not a new problem for either the intelligence or law enforcement communities. When wiretapping the phone of any target – be it the NSA targeting a foreign terrorist or the FBI obtaining a law enforcement warrant to tap the phone of an organized crime figure – it is inevitable that conversations will be overheard with "incidental interceptees," individuals who are not the original targets but who might disclose information of interest.

The concerns about how to police this in practice are understandable, yet it is difficult to come up with a strict quantitative or other bright line test on such matters. You should rest assured that I intend to work closely with the Department of Justice, the DNI's Office of General Counsel, and the offices of general counsel of the agencies involved to develop further training and guidance in this area as needed, to safeguard against reverse targeting and protect privacy and civil liberties. It is important to recognize, also, that reverse targeting makes little sense as a

[4] In *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), the court "adopt[ed] the foreign intelligence exception to the warrant requirement for searches targeting foreign powers (or their agents) which are conducted abroad." See also *United States v. Duggan*, 743 F.2d 59, 71 (2d Cir. 1984) (citing cases); *United States v. Marzook*, 435 F. Supp. 2d 778 (E.D. Ill. 2006) (upholding 1993 physical search under section 2.5).

[5] The court in *United States v. Bin Laden*, 126 F. Supp. at 282 n.23, also noted that it did "not take issue with the policies and procedures" of section 2.5.

matter of intelligence tradecraft: if intelligence officers are indeed interested in a target inside the United States, they will have a natural incentive to seek a FISA court order in any event so as to obtain all of that person's communications, rather than the limited subset that would otherwise be acquired through such reverse targeting.

Are minimization procedures protecting the privacy and civil liberties of U.S. persons?

As discussed above, when the communications of persons overseas are acquired, it is inevitable that some of those communications will incidentally involve U.S. persons. Again, this is a familiar challenge for the Intelligence Community. In general, "minimization procedures" are procedures for reviewing, handling, and, as appropriate, destroying, information about U.S. persons, depending on whether or not the information constitutes foreign intelligence information or fits within another category the agency is authorized to retain. The FISA statute fully embraces and incorporates the concept of minimization as a way of dealing with the inevitability of incidentally intercepting communications of U.S. persons during authorized FISA surveillance.[5]

The Protect America Act requires that similar minimization procedures be followed with respect to surveillance conducted under the Act. These minimization procedures are intended to protect the privacy and civil liberties of U.S. persons who may be communicating with targets overseas. The Act requires that these procedures meet the definition of "minimization procedures" under FISA. My office, the Department of Justice, and the DNI's Office of General Counsel, have reviewed the minimization procedures, and, as part of our periodic compliance assessments, are reviewing compliance with those procedures. These procedures have been made available to the Intelligence Committees. Although not required by the Protect America Act, it should be noted that NSA is using minimization procedures previously reviewed and approved by the Foreign Intelligence Surveillance Court.

Because the minimization procedures used for the Protect America Act are themselves classified, it may be helpful in this unclassified letter to review those procedures for collecting, retaining, and disseminating U.S. person information in place at NSA, that have been released in

---

[5] FISA defines "minimization procedures" as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

unclassified form. While these minimization procedures are not identical to the ones used for the Protect America Act, they provide general guidance for the types of processes and requirements involved with minimization.

United States Signals Intelligence Directive 18 (USSID 18) implements the requirements of Executive Order 12333 for the signals intelligence system. USSID 18 states plainly that "The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. government." (§ 1.1). While some portions of the USSID are classified because they reveal sensitive sources and methods, most of it is unclassified and it has been periodically released under the Freedom of Information Act.[7] USSID 18 applies specific rules for retention, processing, and dissemination of any for communications that are to, from or about U.S. persons:

- Such communications may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement (§ 6.1.a(1));

- Intelligence reports from such communications are written "so as to focus solely on the activities of foreign entities and persons and their agents." (§ 7.1)

- Identities of U.S. persons are generally redacted from intelligence reports and replaced with generic terms such as "U.S. person" or "U.S. firm." Deleted identities are retained for a maximum of one year. (§ 7.1)

- U.S. person identities may generally be released only where the U.S. person has consented to such release, the information about the U.S. person is publicly available (e.g., a foreign target discussing a news report), or the identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance (§ 7.2).

- The USSID lists specific responsibilities, including regular inspections, reports, legal reviews, and training for the Inspector General, General Counsel, and Deputy Director for Operations. Violations must be reported on a quarterly basis to the President's Foreign Intelligence Advisory Board through the Assistant to the Secretary of Defense for Intelligence Oversight. (§ 8).

USSID 18 also contains standard minimization procedures for surveillance conducted by NSA pursuant to the Foreign Intelligence Surveillance Act. These procedures supplement the standard USSID 18 procedures for all signals intelligence activities. They apply substantially the same process, with a few additional safeguards, notably that:

- The acquisition must be made in a manner "designed to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance." (App. 1, § 3(a)).

[7] A redacted version is available from the National Security Archive, a non-profit organization affiliated with George Washington University, at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm

- The lines or numbers being targeted must be verified as the lines or numbers authorized, and collection personnel must, at regular intervals, confirm "that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance." (App. 1, § 3(b)).

In sum, the Protect America Act puts in place privacy and civil liberties protections (1) to help ensure the targets of surveillance are located outside the United States, and (2) to minimize information that is not necessary to understand foreign intelligence or assess its importance in communications to, from or about U.S. persons.

Other Questions

Questions have also been raised about other potential uses – and mis-uses –of authorities granted under the Protect America Act. On September 14, Assistant Attorney General Kenneth Wainstein explained why the Protect America Act does not authorize – among other things – reverse targeting, surveillance of domestic communications that merely "concern" a foreign target, physical searches of Americans' homes, effects or mail, or obtaining Americans' medical or library records. The oversight mechanisms outlined below will help ensure that the Protect America Act is being applied in a manner consistent with those interpretations.

Questions might also be raised as to whether the Protect America Act could enable the Intelligence Community to conduct surveillance for non-intelligence purposes. The requirement that surveillance under the Protect America Act be for "foreign intelligence" purposes also would prohibit abusing such authority for surveillance of Americans' political, religious, or any other domestic activities. Moreover, the provisions of Executive Order 12333 and each agency's Attorney General-approved procedures have for decades required that agencies demonstrate a valid mission-related purpose for collecting, retaining, or disseminating information about a U.S. person.

Other Offices and Institutions Involved in Oversight

While my office takes its oversight responsibilities very seriously, as discussed throughout this letter, it is not alone. As described in more detail in the September 5, 2007 letter of Principal Deputy Assistant Attorney General Brian Benczkowski, the Department of Justice, through the National Security Division, and the Director of National Intelligence, through my office and the DNI's Office of General Counsel, are conducting reviews of the implementation of the Protect America Act. These reviews started within 14 days of the initiation of collection under the Protect America Act and every 30 days thereafter. I am conducting these reviews together with the ODNI's Office of General Counsel and the National Security Division of the Department of Justice.

The following other offices and institutions, in all three branches of government, have a direct role in oversight of the Protect America Act – this list is not exhaustive:

Executive Branch, within the Intelligence Community:

- The Inspector General of the NSA conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures – it is also conducting an audit of the implementation of the Protect America Act;

- The General Counsel of the NSA provides legal advice and assistance and performs oversight in accordance with USSID 18 and the Protect America Act. It also helped develop the training courses on USSID 18 and the Protect America Act and supports administration of the training to the NSA workforce;

- The Signals Intelligence Directorate Oversight and Compliance Office provide oversight and compliance for the implementation of the Protect America Act at NSA;

- Other agency offices of general counsel and offices of inspector general perform similar oversight roles with respect to their agencies' use of this authority;

- The Office of General Counsel of the ODNI provides legal advice and assistance to the DNI in making his certifications under the Act, in assessing compliance with the procedures, an in reporting those assessments to Congress.

Executive Branch, outside the Intelligence Community:

- The Justice Department's National Security Division is conducting compliance assessments, as it does with respect to other FISA authorized activities;

- The Justice Department's National Security Division, the Office of Legal Policy and the Office of Legal Counsel are providing policy and legal advice with respect to the Protect America Act;

- The Justice Department's Civil Liberties and Privacy Office is consulting with the National Security Division in its assessments under the Protect America Act;

- The Privacy and Civil Liberties Oversight Board, currently within the Executive Office of the President, is conducting its own review of the policies and procedures of the Protect America Act;

- The Assistant Secretary of Defense for Intelligence Oversight reviews reports of violations by NSA, and other Defense Department intelligence entities, on a quarterly basis;

- The Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board receives reports of violations on a quarterly basis;

- The DoD Office of Inspector General also conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures.

Legislative Branch

- The Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate are conducting intensive oversight of the Protect America Act.

- Members and staff have engaged in multiple oversight visits at the NSA;

- Both committees have held open and closed hearings on the subject, and have received numerous staff and member briefings.

- The House and Senate Judiciary Committees have likewise received oversight briefings, have conducted oversight visits, and have held public hearings.

- Congress will have an opportunity to revisit and clarify language in the Protect America Act before extending the Act or making it permanent.

Judicial Branch

- The Foreign Intelligence Surveillance Court has a direct role under the statute in reviewing procedures by which the Intelligence Community determine that a target is outside the United States.

- These procedures have already been submitted to the court and are currently under review.

- A recipient of a directive under section 105B of the Protect America Act may challenge its legality before the Foreign Intelligence Surveillance Court.

This extensive oversight helps ensure that agencies implementing the authorities of the Protect America Act are doing so in a careful, thoughtful, way that is fully transparent to the Congress, and that demonstrates due regard for the protection of privacy and civil liberties of Americans.

I hope this information is helpful. If you have any questions or would like more information on any of these issues, please contact Kathleen Turner in the Office of Legislative Affairs at [redacted]

Sincerely,

Alexander W. Joel

SHELDON WHITEHOUSE
RHODE ISLAND

COMMITTEES
AGING
BUDGET
ENVIRONMENT AND PUBLIC WORKS
INTELLIGENCE
JUDICIARY

United States Senate

WASHINGTON, DC 20510-3905

http://whitehouse.senate.gov
(202) 224-2921
TTY (202) 224-7746
170 WESTMINSTER STREET, SUITE 1100
PROVIDENCE, RI 02903
(401) 453-5294

July 27, 2007

RECEIVED
15 Aug 07
Sec

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

Dear Director McConnell:

I appreciated our meeting on July 11, 2007 to discuss the Administration's proposal to modernize the Foreign Intelligence Surveillance Act (FISA). I found your presentation thoughtful and helpful. As you know, Chairman Rockefeller and Chairman Leahy have underscored our need to review the determinations and legal opinions related to the President's Terrorism Surveillance Program in order to proceed with revision to existing U.S. law. This review is critical to a careful revision of the FISA that satisfies our national security needs and addresses important civil liberties concerns.

During our meeting, you singled out three key changes to the FISA that you would like to be enacted on an expedited basis. In our ensuing discussion, we confirmed that one of these provisions is already part of U.S. law. As I noted in our meeting, it is vital to have legislative language that is narrowly crafted to cover your two remaining changes in order to move forward in a timely way. I look forward to reviewing the new language as soon as you develop it.

I welcome the opportunity to continue our dialogue on this important issue. Thank you for your attention to this matter and I look forward to your prompt response.

Sincerely,

Sheldon Whitehouse
United States Senator

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

July 27, 2007

The Honorable Harry Reid
Majority Leader
United States Senate

The Honorable Mitch McConnell
Minority Leader
United States Senate

The Honorable Nancy Pelosi
Speaker
House of Representatives

The Honorable John A. Boehner
Minority Leader
House of Representatives

Dear Majority Leader Reid, Minority Leader McConnell, Madam Speaker, and Minority Leader Boehner:

I appreciate the opportunity for today's meeting between staff members and the constructive dialogue on legislation to modernize the Foreign Intelligence Surveillance Act (FISA) and restore our capability to help defend the country effectively. I am pleased that there appears to be genuine agreement on the need to act before the August recess to close gaps in our current capability.

Congressional staff provided thoughts on possible modifications of the current FISA court process as an interim solution to remedy this gap. Unfortunately, this proposal would not close critical gaps in the Intelligence Community's ability to provide warning of threats to the country. The proposal would continue the current situation that, in a significant number of cases, we would have to obtain court orders to collect foreign intelligence about foreign targets located overseas. The proposal would also require in practice that we continue to divert scarce counterterrorism experts to compiling court submissions in order to gain judicial approval to gather necessary foreign intelligence about these overseas targets. I conclude this proposal would not solve the deep concerns I have expressed about the current situation facing the country.

Attached is an interim proposal which I believe will effectively close the critical gaps in our intelligence capability in the short term. Although my strong preference is the immediate adoption of the proposal I transmitted to Congress in April, in light of the urgency of the

situation, I offer the attached significantly narrowed proposal focused on the current, urgent need of the Intelligence Community to provide warning. The proposal would make clear that court orders are not necessary to effectively collect foreign intelligence about foreign targets overseas. The proposal would also provide a means of obtaining assistance that may be required from private parties.

It is also my strong preference that we immediately provide liability protection for those who are alleged to have assisted the government following September 11, 2001. However, in recognition of your indication that more time is necessary to consider this matter, the interim proposal does not contain such a provision. While far from ideal, this interim proposal would immediately give our Intelligence Community the tools it needs to protect the Nation, pending continued discussion of this important additional issue.

I am available to brief all members of the Congress at their earliest convenience on this matter. I look forward to continuing our discussions and constructive dialogue. If you have any questions on this matter, please contact me or the Chief of Staff to the President.

Sincerely,

J.M. McConnell

cc: The Honorable John D. Rockefeller IV
The Honorable Christopher S. Bond
The Honorable Silvestre Reyes
The Honorable Peter Hoekstra
The Honorable Patrick J. Leahy
The Honorable Arlen Specter
The Honorable John Conyers, Jr.
The Honorable Lamar S. Smith

Attachment: As stated

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

July 24, 2007

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

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

The Honorable Carl Levin
Select Committee on Intelligence (Ex-Officio)
United States Senate
Washington, DC 20510

Dear Senators:

Thank you for meeting with the Chief of Staff to the President, the Counsel to the President, and me on Monday, July 23, 2007 to discuss a way forward on legislation to modernize the Foreign Intelligence Surveillance Act (FISA) so as to restore our capability to help defend the country effectively. I appreciate the opportunities provided by the Senate over the past months to discuss the urgency of my proposal given the threat faced by the country.

Given the constructive dialogue of the past months, I was disappointed in the indication at the meeting that the Senate may not be able to act on legislation before the August recess. The recently released National Intelligence Estimate concluded that the United States currently "is in a heightened threat environment." I have briefed a majority of Senators on specific details that cause me to have deep concern about the current threat facing the country.

I have also discussed at hearings and other meetings how outdated parts of the FISA statute significantly degrade the capability of the Intelligence Community to collect critical intelligence to protect America, while doing little to enhance privacy protections for Americans. As you are aware, in a significant number of cases, we are in the unfortunate position of having to obtain court orders to collect foreign intelligence about foreign targets located overseas.

My duty as head of the Intelligence Community is to provide warning of terrorist activity and other threats to our security. But under the current statute, we are missing a significant amount of foreign intelligence that we should be collecting to protect our country. I will soon

forward separately a classified attachment to this letter describing the degraded capability we currently face as a result of various developments and the reason for my deep concern.

In my view, it is essential to our Nation's security that Congress act immediately to modernize FISA. The Administration's strong preference is the immediate adoption of our proposed bill, including retrospective protection against lawsuits for those who are alleged to have assisted the government. In our conversations, you have indicated that the most significant impediments to prompt action on legislation are the Administration's insistence on retrospective immunity for those who are alleged to have assisted the government after September 11, 2001 and the Administration's unwillingness to provide certain documents related to highly classified intelligence programs, particularly historical information on such programs. While I would strongly prefer the liability issue be taken up and resolved now, my highest priority must be to ensure that I am able to close intelligence gaps and provide critical warning time for our country. If you continue to believe that it is not possible to resolve all issues prior to the August break, then I strongly urge you as a first step to act immediately on a FISA modernization bill that would be prospective only. Our work during the summer recess could then turn to identifying a way to provide meaningful liability protection and to attempt to reach an accommodation on the document requests. While far from ideal, the Administration would support such a bifurcated process that would allow us to modernize FISA immediately and give our Intelligence Community the tools it needs now to protect the Nation, while leaving aside the important but less urgent liability and document issues until later in the summer.

In the context of the current threat, the most critical piece needed right now by the Intelligence Community is FISA modernization. I urge you to act prior to the August recess to ensure we do not have critical gaps in our ability to provide warning of threats to the country. As I stated before the Senate Select Committee on Intelligence on May 1, 2007, "[w]e must make the requested changes to protect our citizens and the nation."

I look forward to continuing our discussions. If you have any questions on this matter, please contact me or the Chief of Staff to the President.

Sincerely,

J.M. McConnell

cc: The Honorable Christopher S. Bond
The Honorable Arlen Specter
The Honorable John McCain

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JUN 25 2007

The Honorable Tom Udall
House of Representatives
Washington, DC 20515

Dear Representative Udall:

Thank you for your May 3, 2007 letter to the President regarding Title IV of the Administration's proposed Intelligence Authorization Act for Fiscal Year 2008. The President has asked me to respond to your concerns regarding the proposed amendments to the Foreign Intelligence Surveillance Act (FISA). It is vitally important that Congress and the Executive Branch work together to close critical gaps in our intelligence capability, while ensuring the protection of the civil liberties of Americans.

As you have observed, in certain emergency situations, the proposed amendment to FISA would permit the retention of information if it "contains significant foreign intelligence information." The intent behind the provision is to ensure that the Government may retain valuable foreign intelligence that is collected unintentionally, rather than being required to destroy all such information. However, this provision would not allow all information inadvertently collected to be retained. Rather, the Government could retain only significant information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, to include information on international terrorist activities. As a safeguard, the Administration's proposal would require that all such retention be regularly reported to the congressional intelligence committees as part of the Attorney General's assessments currently required by FISA.

The proposal, as you note, also contains liability protection for persons that allegedly assisted the government with lawful intelligence activities after September 11, 2001. We appreciate your position; however, it is vitally important that the Government retain a means to secure the assistance of private parties. As a former Director of the National Security Agency, a private sector consultant to the Intelligence Community, and now the Director of National Intelligence, I am acutely aware that in order for us to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

We appreciate your input regarding the specifics of the proposal. We have begun a constructive dialogue with Members of Congress, their staffs, and groups outside of government to discuss concerns and ideas for modifications. We are sure you agree that 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.

If you have any questions on this matter, please contact my Director of Legislative Affairs Kathleen Turner, who can be reached on [redacted]

Sincerely,

J. M. McConnell

Sir, I also would be happy to meet with you personally to discuss further.

V/R

JMc

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

July 25, 2007

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

Dear Chairman Reyes:

I write in response to your letter to the President of July 18, 2007, in which you stress the imperative of the President's taking steps to protect the Nation in light of recent findings regarding terrorist risks to our homeland. I appreciate the commitment in your letter to make immediate changes to the Foreign Intelligence Surveillance Act (FISA) if clarifications to the law were necessary. I am writing to reiterate my belief that such clarifications are urgently needed and are reflected in the FISA modernization proposal that the Administration has submitted to Congress. I hope that Congress will be able to act immediately, as your letter suggests, to provide the legislative changes needed to protect the nation in this period of heightened threat.

As you note, our Nation faces an intelligence "gap"— a situation in which our Intelligence Community everyday is "missing a significant portion of what we should be getting" in order to protect the American people. I stressed the same point in recent testimony before the Senate by explaining that "[w]e must make the requested changes [to FISA] to protect our citizens and the nation" because, under FISA today, "[w]e are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States." Put differently, as the head of our Nation's Intelligence Community, I am obligated to provide warning of threats of terrorist activity and I have deep concern about the current threat situation.

Like you, I believe that this situation is unacceptable in the current, heightened threat environment. The recent National Intelligence Estimate concluded that our Nation faces a determined enemy in Al Qaeda. If we are to stay a step ahead of the terrorists and protect the American people, I firmly believe that we need to be able to use our capabilities to collect foreign intelligence about foreign targets overseas without requirements imposed by an out-of-date FISA statute. Accordingly, I share your view that it is essential that the Administration and Congress work together and without delay to close the current intelligence gap by amending the FISA statute.

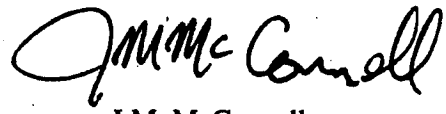
Hearings before the House Permanent Select Committee on Intelligence (HPSCI) in 2006 discussed this gap, in addition to open and closed hearings before the Senate in 2006. See, for example, Lt. General Alexander's statement before the Senate Judiciary Committee on July 26,

2006 at a hearing on "FISA for the 21st Century." While these hearings have resulted in discussion of the issues, FISA remains in need of modernization. Today, for instance, the statute requires in a number of important situations that we obtain court orders to most effectively obtain foreign terrorist communications. Simply put, in a significant number of cases, we are in the unfortunate position of having to obtain court orders to effectively collect foreign intelligence about foreign targets located overseas.

Let me also emphasize that Congress's providing additional resources to the Executive Branch will not remedy intelligence gap. It is necessary and essential that Congress modernize FISA. I believe it is not feasible, nor is it wise, to remove significant numbers of our most critical analytic resources – counterterrorist analysts who understand the languages, organization, and operations of our enemies – from tracking current threats to the nation and devote large numbers of them to writing detailed probable cause justifications in cases where the foreign targets are located overseas. The classified annex outlines the scope of the issue and explains in more detail why providing additional resources are not the answer. In short, resource allocation is not the fundamental issue we face in this area, but instead a fundamental problem with a law that requires modification to ensure we are protecting America, while respecting the privacy rights of Americans.

Please contact me if you have any questions or additional views on how to amend FISA immediately.

Sincerely,



J.M. McConnell

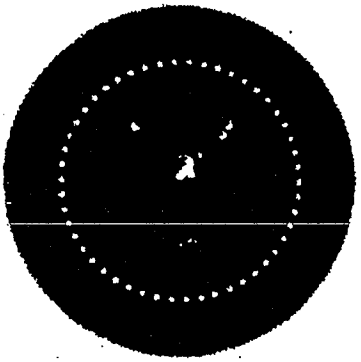
cc: HPSCI members

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

UNCLASSIFIED
STATEMENT FOR THE RECORD

INTRODUCTION

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

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.

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 as a tool to gather foreign intelligence information more quickly and efficiently.

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.

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.

Some of the specifics that support my testimony cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose capability. I look forward to elaborating further on all aspects of the issues in a closed, classified setting.

I can, however, make a summary level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation.

TODAY'S NATIONAL SECURITY THREATS

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 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.

Today, 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.

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.

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.

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.

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

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?

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

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.

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.

Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.

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 technology.

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, certain 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."

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.

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

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

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, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: there are circumstances under which when 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 this collection. We find ourselves in this position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

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 person, 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.

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.

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 persons. 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.

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.

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 they have been for decades.

SECURING ASSISTANCE UNDER FISA

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.

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.

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

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.

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

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.

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.

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.

With this robust oversight structure in place, it also is important to 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.

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.

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

This proposed legislation seeks to accomplish several goals:

- 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.

- 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.

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

- 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 FISA process, streamlining the FISA process makes for better government.

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.

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.

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.

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

Congress of the United States
Washington, DC 20515

August 1, 2007

The Honorable Michael McConnell
Director of National Intelligence
Bolling Air Force Base
Washington, DC 20005

Dear Admiral McConnell:

Thank you for meeting with the Blue Dogs yesterday.

We share your concern about the need for surveilling all foreign-to-foreign communications involving suspected terrorists, and believe Congress should act before we recess to clarify your authority to do this.

We support legislation to:

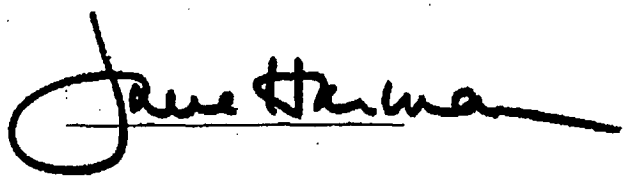
1. Authorize the FISA Court to issue a single order which approves your ability to conduct certain targeting operations in foreign countries.
2. Clarifies that no court order is required to conduct surveillance of foreign-to-foreign communications that are routed through the United States.
3. Requires individualized warrants for Americans.
4. Compels compliance by private sector partners.
5. Sunsets in 180 days.

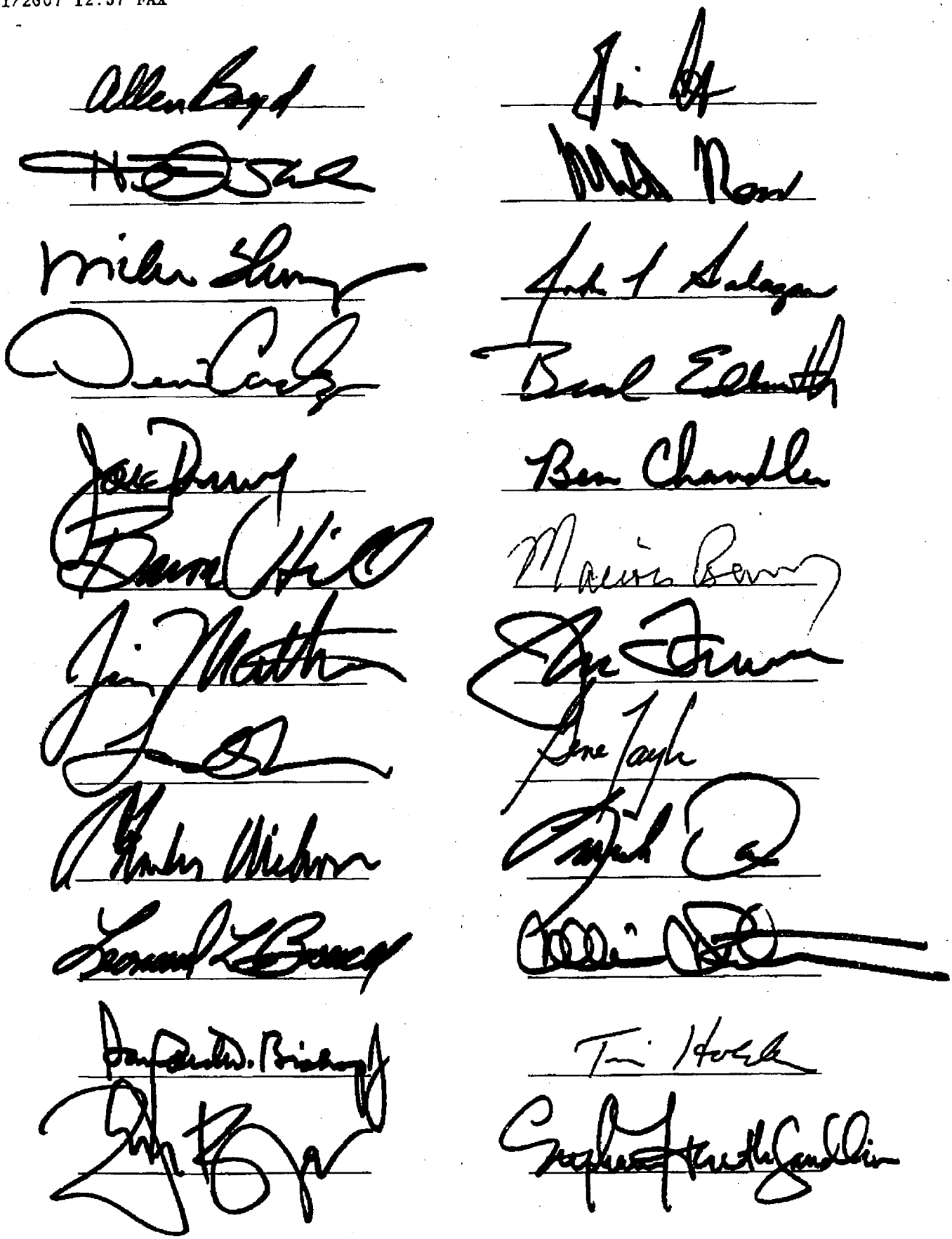
We also agree that it is important to address the issue of retroactive liability for private sector partners.

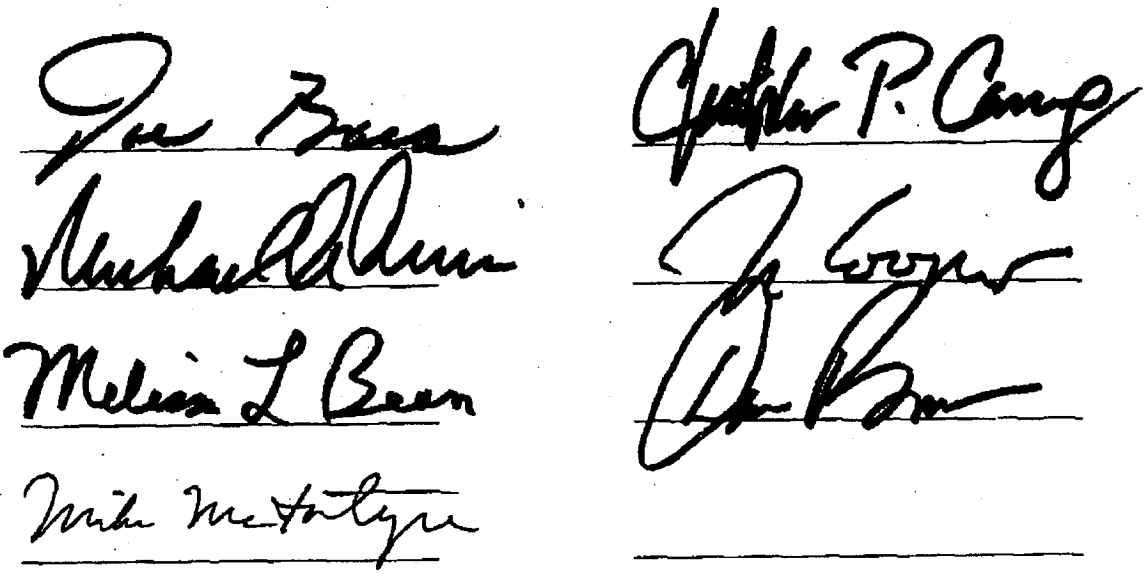
We intend to communicate our views promptly to House leadership and to urge them to put this legislation on the House Calendar this week.

Sincerely,

Bud Cramer





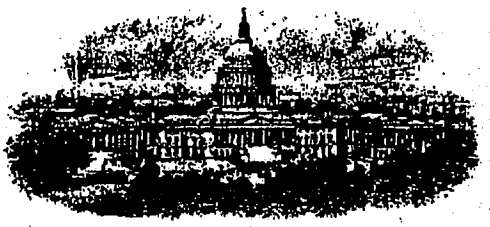


BUD CRAMER
5TH DISTRICT
ALABAMA

COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEES
DEFENSE
TRANSPORTATION, HOUSING AND URBAN DEVELOPMENT, AND RELATED AGENCIES
FINANCIAL SERVICES AND GENERAL GOVERNMENT

SELECT INTELLIGENCE OVERSIGHT PANEL

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
SUBCOMMITTEES
OVERSIGHT AND INVESTIGATIONS
TECHNICAL AND TACTICAL INTELLIGENCE



Congress of the United States
House of Representatives
Washington, D.C. 20515

FACSIMILE COVER SHEET

OFFICES:
2184 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4801

200 PRATT AVENUE NORTHEAST
SUITE A
HUNTSVILLE, AL 35801
(256) 551-0190

MORGAN COUNTY COURTHOUSE
BOX 668
DECATUR, AL 35602
(256) 355-9400

THE BEVILL CENTER
1011 GEORGE WALLACE BOULEVARD
TUSCUMBIA, AL 35674
(256) 381-3450

E-mail: budmail@mail.house.gov
Web page: http://cramer.house.gov

If you have any problems or questions regarding this transmission, please contact (202) 225-4801.

TO: Admiral McConnell

FROM: Rep Cramer

DATE:

FAX #: [redacted]

# of Pages (including cover): 4

Notes:

This mailing was prepared, published, and mailed at taxpayer expense.
Printed on recycled paper with soy ink.

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

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

MK:HAELDEIANEY
ETAFFDWECTOR

MICHAELMEERMANG
MINORITYSTAPFDIRECTOR

May 31, 2007

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

The Honorable Alberto Gonzales
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Director McConnell and General Gonzales,

The House Permanent Select Committee on Intelligence is conducting a review of electronic surveillance activities by U.S intelligence agencies and legal authorities governing electronic surveillance, particularly the Foreign Intelligence Surveillance Act (FISA).

This letter follows previous letters sent by the Committee as well as several requests made by Members and Staff for documents relating to the NSA Surveillance Program, described by the President as the "Terrorist Surveillance Program," (hereinafter, the Program).

To assist the Committee in evaluating arguments about the need to alter FISA, we request that you provide the following documents to the Committee no later than June 8, 2007.

1) All documents that reflect the President's authorization and reauthorization of the Program, including any predecessor or successor programs, from 2001 to present;

2) Any policy decision memorandum - or like document - that details the policy rationale for the President's authorization of the original Program. If such memoranda cannot be provided, a written statement, signed by competent authority, detailing the need for the TSP authorization in 2001 will suffice;

3) All documents, including memoranda, that contain analysis or opinions from the Department of Justice, the National Security Agency, the Department of Defense, the White House, or any other entity within the Executive Branch on the legality or legal basis for the Program, including documents that describe why the necessary surveillance could or could not take place under FISA, from 2001 to present;

4) Any memorandum within the control of the Executive Branch that details the civil liberties safeguards (including minimization procedures) for American citizens built into Program from 2001 on, also any memorandum that explains the efficacy of such civil liberties safeguards. If such memoranda cannot be provided, a written statement, signed by competent authority, explaining these safeguards and their efficacy will suffice;

5) A written assessment of the efficacy of the Program from 2001 on. Such assessment should explain what kind of information was gained by the Program, how effective the Program was in gaining such information, what that information was used for and the relative value of continuing the Program in its current form;

6) All documents that reflect communications with the Foreign Intelligence Surveillance Court about the Program or types of surveillance that were conducted as part of that Program, that contain legal analysis, arguments, or decisions concerning any interpretation of FISA, the Fourth Amendment, the Authorization to Use Military Force or the President's authority under Article II of the Constitution, from 2001 to the present;

7) A written assessment of the effects of the unauthorized public disclosure of the Program in December 2005. Such assessment should include a statement of the impacts of the unauthorized disclosure in terms of fiscal costs, continued access to intelligence information, cooperation of third parties and overall harm to U.S. national security;

8) All documents that reflect communications with any telecommunications company relating to the authorization, legal authority, or legal justification for the Program, from 2001 to present."

The Committee cannot begin a serious evaluation of legislative proposals to alter the FISA system unless we have facts regarding the adequacy of existing legal authorities. We trust that you will comply with this request so that our evaluation of legislation may begin promptly.

Sincerely,

estre Re s
Chairman

Peto Hoekstra
Ranking Republican Member

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

August 6, 2007

The Honorable Harry Reid
Majority Leader
United States Senate

The Honorable Mitch McConnell
Minority Leader
United States Senate

Dear Majority Leader Reid and Minority Leader McConnell:

I write to the United States Senate after discussions with Members indicated a letter discussing the "Protect America Act of 2007," S.1927 (Act) would be helpful. I deeply appreciate the time spent by Members understanding the need for this legislation and acting before the August recess to close critical gaps in the Intelligence Community's ability to provide warning of threats to the country.

First, I note that this was not an issue discussed only in the last few weeks. In 2006, there were extensive hearings and meetings before the Senate and the House of Representatives, including an unusual open hearing before the Senate Judiciary Committee on "FISA for the 21st Century" on July 26, 2006 where the Director of the Central Intelligence Agency and the Director of the National Security Agency (NSA) testified. In addition, there were numerous bills introduced in both the House and Senate. Indeed, in 2006, the House of Representatives passed the "Electronic Surveillance Modernization Act" (H.R. 5825), but the Senate did not pass legislation on this issue. In April 2007, responding to a congressional request, I transmitted to Congress a proposal to modernize FISA and appeared at an open hearing before the Senate Select Committee on Intelligence on May 1, 2007.

In addition, there were numerous classified briefings provided to committees of Congress, individual Member briefings, and sessions open to all Members of Congress. The legislative record of consideration of this issue has been lengthy and deep in substance.

Second, there is understandable confusion in the public discussion of what is admittedly a complex – and frequently classified – issue. But I would note that in the interest of providing an extensive legislative record and allowing for public discussion of this issue, the Intelligence Community discussed in open settings extraordinary information dealing with our operations. This will come at a price to our ability to collect vital foreign intelligence. However, to ensure there was open legislative consideration of this matter, leaders of the Intelligence Community went far further in open discussions than in any other time I can recall in my forty-year intelligence career.

As I noted in my testimony on May 1, 2007, but lost in some recent discussion of this issue, the fundamental fact is that the Act is aimed at restoring the effect of the Foreign Intelligence Surveillance Act (FISA) drafted in 1978. FISA, based on the technology of 1978,

specifically excluded from its scope certain types of international communications carried by radio and satellite. Today, many of those same communications are now transmitted by different means. This change in technology resulted in requiring, in a significant number of cases, that the Government seek court orders to monitor the communications of foreign persons physically located in foreign countries. To be clear -- the Intelligence Community was diverting scarce counterterrorism analysts who speak the languages and understand the cultures of adversaries to compiling lengthy court submissions to support probable cause findings on an individualized basis by the FISA Court in order to gather foreign intelligence from foreign terrorists located overseas. This is an unacceptable and irresponsible use of Intelligence Community resources.

Related to the discussion of exclusions contained in FISA as enacted in 1978 is the proposal of limiting the gathering of foreign intelligence from targets located overseas to discrete categories such as "international terrorism." In 1978, generally no such limitation was placed on activities excluded from the definition of electronic surveillance in FISA and directed at persons overseas -- nor is one appropriate today. The Intelligence Community must be able to gather needed intelligence information on the array of threats to our national security as it was able to in 1978.

Third, while fixing the problems created by changes in technology, the Act creates new requirements not present in FISA as enacted in 1978. In addition to requiring certain determinations from the Attorney General and the Director of National Intelligence, the Act requires the Government to submit its procedures established under the Act for determining that acquisitions are not electronic surveillance to the FISA Court for judicial review.

Fourth, FISA – both before the enactment of this Act and after – generally requires a court order to target the communications of persons in the United States for electronic surveillance as defined by FISA. Again, that was the case before this enactment and will remain the case after. This is a requirement I strongly support.

Fifth, there has also been confusing discussion about the treatment of information concerning United States persons by NSA. These procedures governing how NSA treats information concerning United States persons are frequently referred to as "minimization" procedures. During the course of normal operations, NSA will sometimes encounter information to, from or about U.S. persons. That fact does not, in itself, cause FISA to apply to NSA's activities directed at persons located overseas.

Instead, as it has for decades, NSA applies procedures approved by the U.S. Attorney General to its activities that minimize the acquisition, retention, and dissemination of information concerning U.S. persons. These procedures have worked well for decades and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

The Act makes clear in Section 105B(a)(5) that "the minimization procedures to be used with respect to [acquisitions must] meet the definition of minimization procedures under section 101(h)" of FISA, which defines in law the requirements of such procedures. The Act does not change the definition of minimization procedures contained in FISA.

Finally, there will be intense oversight of activities conducted under the Act. There are extensive training, compliance, and other procedures in place at agencies to ensure our activities

are conducted according to law. The relevant agencies have Inspectors General staffs with the appropriate clearances, training, and technical background to ensure that activities are reviewed and audited.

I am committed to keeping the Congress fully and currently informed of how this Act has improved the ability of the Intelligence Community to protect the country and reporting – and remedying – any incidents of non-compliance.

Thank you for the time afforded to me and the consideration of proposals to fix critical gaps in our intelligence operations. I look forward to continuing our discussions and working with all Members to address any concerns about the Act. If you have any questions on this matter, please contact me.

Sincerely,

J.M. McConnell

cc: All Senate Members

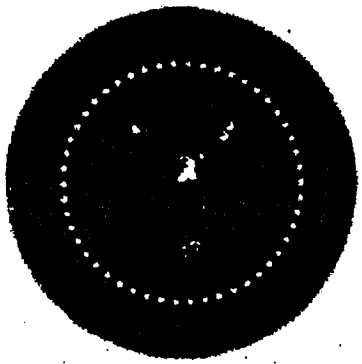
Attachment: DNI Statement for the Record, May 1, 2007

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

UNCLASSIFIED
STATEMENT FOR THE RECORD

INTRODUCTION

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

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.

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 as a tool to gather foreign intelligence information more quickly and efficiently.

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.

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.

Some of the specifics that support my testimony cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose capability. I look forward to elaborating further on all aspects of the issues in a closed, classified setting.

I can, however, make a summary level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation.

TODAY'S NATIONAL SECURITY THREATS

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 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.

Today, 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.

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.

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.

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.

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

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?

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

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.

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.

Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.

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 technology.

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, certain 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."

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.

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

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

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, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: there are circumstances under which when 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 this collection. We find ourselves in this position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

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 person, 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.

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.

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 persons. 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.

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.

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 they have been for decades.

SECURING ASSISTANCE UNDER FISA

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.

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.

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

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.

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

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.

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.

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.

With this robust oversight structure in place, it also is important to 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.

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.

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

This proposed legislation seeks to accomplish several goals:

- 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.

- 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.

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

- 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 FISA process, streamlining the FISA process makes for better government.

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.

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.

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.

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE
(ACTING)
WASHINGTON, DC 20511

SEP 27 2007

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

Dear Mr. Chairman:

Thank you for your letter of September 24, 2007 to the Director of National Intelligence (DNI) regarding the discussion at your Committee's hearing on the Protect America Act and an incident in which proceeding under the Foreign Intelligence Surveillance Act (FISA) to collect on foreign targets abroad delayed the initiation of coverage expected to reveal the communications of Iraqi insurgents who had kidnapped U.S. soldiers. By providing this event as an example, the DNI hoped to provide some context as to why the authorities provided by the Protect America Act are critical to protect the nation.

In particular, in the hearing before the House Judiciary Committee on September 18, 2007, the DNI provided the following example: "American soldiers [were] captured in Iraq by insurgents, and we found ourselves in a position where we had to get a warrant to target the communications of the insurgents." The DNI explained that the process of obtaining a court order put the Intelligence Community (IC) in a difficult position.

In the hearing before your Committee on September 20, 2007, the DNI was asked to discuss this example further. In that testimony, the DNI explained that this example demonstrated that FISA has put us in a position where "[w]e are extending Fourth Amendment rights to a terrorist foreigner, foreign country, who's captured U.S. soldiers, and we're now going through a process to produce probable cause...." The Director further explained the greater context, which is that FISA, because it has not kept pace with technology, requires that the IC meet a probable cause standard in situations where no substantial privacy right of an American is at issue. Moreover, the DNI endeavored to explain that while useful, the emergency provisions of FISA still require a finding of probable cause that the target of the collection is an agent of a foreign power.

The timeline you have proposed releasing publicly contains a number of additional details that the DNI did not discuss in open session. If you believe that the public release of this timeline will help to further inform the debate, the IC does not object. Indeed, Director McConnell tried to be as open as possible in his testimonies because we understand that these issues are of utmost importance to the Congress and to the public. In the interest of protecting sensitive sources and methods, however, we have made some minor modifications to your original proposal, which are attached.

Some aspects of the proposed timeline also deserve clarification. The timeline that you provided may give the impression that the process of obtaining the emergency authorization

under FISA began at 10:00 a.m. on May 15, 2007. In fact, the process began earlier, as evidenced by the source material provided to the Committee by the National Security Agency on June 8, 2007. On May 14, 2007, 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.

As the Committee is aware, the circumstances of this case presented novel and complicated issues. These issues, which needed to be evaluated before the emergency authorization could be requested, distinguished this situation from a typical case of targeting non-U.S. persons abroad. This was the focus of the internal Executive Branch deliberations between 12:53 p.m. and 5:15 p.m. and the reason behind the decision to contact the Attorney General for emergency authority rather than the Solicitor General.

While admittedly this was a complex situation, the Director used this example to illustrate the point that, due to changes in technology, the FISA statute extends privacy protections to foreign terrorists located outside the United States merely because FISA makes a geographic distinction based on the location of the collection. Novel issues aside – in order to comply with the law – the Government was required to spend valuable time obtaining an emergency authorization as required by FISA to engage in collection related to the kidnapping.

The Committee has received extensive, in-depth briefings and detailed documentation concerning this case over the past months. The professionals, both in the IC and at the Department of Justice, analyzed the facts and legal issues presented in this situation as they are required to do under the law. FISA's emergency provision, while extremely useful, still requires a determination before the Attorney General can authorize the collection that there is a factual and legal basis for granting FISA authority. Failure to ensure that the facts and the legal issues of this case satisfied FISA's requirements could have exposed these professionals to criminal penalties.[1]

We appreciate the time and effort you have spent on this important issue and we look forward to working with you further to make the authorities provided by the Protect America Act permanent. If you have any questions on this matter, please contact the Director of Legislative Affairs, Kathleen Turner, who can be reached on [redacted]

Sincerely,

Ronald L. Burgess, Jr.
Lieutenant General, USA

Enclosure

cc: The Honorable Peter Hoekstra

[1] See 50 U.S.C. § 1809 (providing criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute).

United States Senate
COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

August 7, 2007

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

Dear Admiral McConnell:

Thank you for your letter of August 6, 2007, regarding S. 1927, the Protect America Act of 2007, which was signed by the President over the weekend.

As you know, the Act is scheduled to sunset in six months, so Congress will be revisiting the issue in the near future. For this reason, I believe it would be very helpful for you to clarify a few additional points regarding the Act and the alternative considered by the Senate.

First, Section 105A of the Foreign Intelligence Surveillance Act (FISA), as added by the Act, would exclude from the definition of electronic surveillance any surveillance directed at a person reasonably believed to be located outside of the United States, presumably even if that person is a U.S. citizen. A number of us have expressed concern about the failure of section 105A to distinguish between foreigners and U.S. persons outside the United States – particularly in light of your repeated statements that your intent was to ensure that the Intelligence Community could "effectively collect foreign intelligence from foreign targets overseas."

Was it your intent that U.S. persons outside the United States be subject to surveillance in the same manner and to the same extent as foreigners? If not, would you agree that Section 105A should be clarified to make this distinction?

Second, when the Act was under consideration in the Senate, Senator Rockefeller and I introduced an alternative bill, S. 2011. In a statement dated August 2, 2007, you indicated that you "could agree to a procedure that provides for court review – after needed collection has begun – of our procedures for gathering foreign intelligence through classified methods directed at foreigners located overseas." S. 2011 takes this approach. In particular:

- Like the bill that was adopted, S. 2011 would permit the DNI and the Attorney General to authorize the immediate electronic surveillance of persons reasonably believed to be outside the United States, without first applying to a court or waiting for court approval. Under S. 2011, the DNI and the Attorney General would be required to submit an application for approval within 10 days of initiating electronic surveillance and could continue surveillance pending a ruling by the court. Even if the court ruled that the procedures were invalid, the surveillance could continue (with the court's approval) during the pendency of any appeal.

- Like the bill that was adopted, S. 2011 would not require the FISA court to review applications for the use of electronic surveillance in specific cases. Instead, the FISA court would review procedures certified by the DNI and the Attorney General to ensure that electronic surveillance will target persons reasonably believed to be located outside the United States.

While the Rockefeller-Levin approach (S. 2011) was under consideration on the Senate floor, it was represented that you "could not support" it. I have enclosed a copy of S. 2011. I would appreciate if you would review it and let me know whether in fact you oppose it, and if so, what specific language is of concern to you.

Thank you for your willingness to continue to work with us on this important issue.

Sincerely,

Carl Levin
Chairman

TITLE

This Act may be cited as the "Protect America Act of 2007".

SECTION 1. PURPOSE – To provide for a procedure before the FISA Court for an order, which may be amended as necessary at the request of the government with the approval of the Court, authorizing procedures, guidelines, means or methods that will permit the collection of intelligence between foreign persons located outside the United States, while bringing incidental contacts with United States persons at home or abroad into compliance with existing law and minimization procedures.

SECTION 2. ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN ELECTRONIC SURVEILLANCE.

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

"CLARIFICATION OF SURVEILLANCE OF PERSONS OUTSIDE THE UNITED STATES

"SEC. 105A. Notwithstanding any other provision of this Act, a court order is not required for the electronic surveillance of the contents of any communication between persons that are not located within the United States for the purpose of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States..

"ADDITIONAL PROCEDURE FOR COURT APPROVAL FOR AUTHORIZING CERTAIN ELECTRONIC SURVEILLANCE

"SEC. 105B. (a) IN GENERAL.—Notwithstanding any other provision of this title, the Attorney General, in consultation with Director of National Intelligence, upon the authorization of the President, may apply to a judge of the court established under section 103(a) for an ex parte order, or an extension of an order, authorizing electronic surveillance for a period of 1 year, in accordance with this section.

"(b) APPLICATION.—

"(1) CONTENTS.—An application for an order, or extension of an order, submitted under subsection (a) shall include—

"(A) the identity of the Federal officer making the application;

"(B) a written certification made under oath by the Director of National Intelligence and the Attorney General that—

"(i) there are reasonable procedures in place for determining that the electronic surveillance under this section is directed at persons reasonably believed to be located outside the United States;

"(ii) there are reasonable procedures in place to assess the implementation of the procedures described in subclause (i) to achieve the objective described in that subclause;

"(iii) the acquisition does not constitute electronic surveillance within the meaning of paragraph (1) or (3) of section 101(f), and, to the extent any acquisition constitutes electronic surveillance within the meaning of paragraph (2) or (4) of section 101(f), that it is approved or minimized as appropriate;

"(iv) a significant purpose of the electronic surveillance is to obtain foreign intelligence information;

"(v) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(vi) the electronic surveillance involves obtaining 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;

''(C) a general description of the nature of the foreign intelligence information sought; and

''(D) a general statement of the means by which the electronic surveillance will be effected.

''(2) SPECIFIC PERSONS AND PLACES NOT REQUIRED.—(A) An application for an order, or extension of an order, submitted under subsection (a) shall not be required to identify—

''(i) the persons, other than a foreign power, against whom the electronic surveillance will be directed; or

''(ii) the specific facilities, places, premises, or property at which the electronic surveillance will be directed or conducted;

''(c) APPLICATION APPROVAL; ORDER.—

"(1) APPLICATION APPROVAL.—Notwithstanding any other law, a judge considering an application for an order, or extension of an order, submitted under subsection (a) shall –

"(A) assess –

"(i) the procedures by which the Government determines that electronic surveillance under this section is directed at persons reasonably believed to be located outside the United States; and

(ii) the minimization procedures to be used with respect to United States persons from such electronic surveillance activity; and

"(B) approve such application if the judge determines that the procedures assessed are in accordance with law and are reasonably designed to determine whether the targets are outside the United States;

"(2) ORDER.—A judge approving an application pursuant to paragraph (1) shall issue an order that—

"(A) (I) authorizes the electronic surveillance as requested, and (ii) approves the minimization procedures with respect to United States persons;

"(B) directs the applicant to follow the procedures referred to in section 105B (b)(1)(B)(I) and the minimization procedures submitted by the Government as approved;

"(C) at the request of the applicant, requires a specified communications service provider, custodian, or other specified person, to furnish the applicant forthwith with all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in a manner that will protect the secrecy of the electronic surveillance and

produce a minimum of interference with the services that provider, custodian, or other person is providing; and

"(D) at the request of the applicant, requires such communications provider, custodian, or other specified person to maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the electronic surveillance or the aid furnished that such person wishes to maintain.

"(3) MINIMIZATION PROCEDURES.An application for reauthorization of an order issued under this section, shall contain a description of the Government's minimization procedures.

"(d) GUIDELINES FOR SURVEILLANCE OF UNITED STATES PERSONS. – Not later than 15 days after the date of the enactment of this section, the Attorney General shall establish guidelines that address communications with persons inside the United States and United States persons outside the United States and are designed to ensure that an application is filed under section 104 when the Attorney General seeks to continue electronic surveillance that began under this section but:

"(1) effectively is or has become surveillance of a person within the United States; or

(2) is of a nature or quantity as to infringe on the reasonable expectation of privacy of persons within the United States.

"(e) COMPENSATION.—The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to an order of the court under this section or pursuant to a directive under section 105C.

"(f) LIABILITY.—Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with an order under this section or a directive under section 105C.

"(g) RETENTION OF ORDERS.—An order granted under this section and directives under section 105C shall be retained for a period of not less than 10 years from the date on which such order or directive is made."

"(h) APPEAL. The Government may appeal any denial of an application submitted under this section to the court established under section 103(b). If such court determines that the denial was properly entered, the court shall immediately provide for the record a written statement of each reason for its decision, and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

"IMMEDIATE AUTHORIZATION OF CERTAIN ELECTRONIC SURVEILLANCE

"SEC. 105C. (a) In General—Notwithstanding any law, the Director of National Intelligence and the Attorney General, may, prior to the submission of an application under section 105B, authorize the immediate electronic surveillance of persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine that it is in the interest of the national security of the United States to begin the electronic surveillance and such electronic surveillance is subject to the certification to be filed as set forth below. The authority in this subsection shall not be used for successive or multiple authorizations of electronic surveillance of the same or similar scope.

"(b) In such a case, the Attorney General shall—

"(1) transmit within 5 days of the initiation of electronic surveillance pursuant to this section under seal to the court established under section 103(a) a copy of a certification made under section 105B(b)(1)(B). 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 except upon motion of the Government;

"(2) submit an application for the approval of such electronic surveillance to the court established under section 103(a) as soon as practicable, but I no event more than 10 days after the initiation of the electronic surveillance;

"(3) the court shall act on such application in accordance with section 105B within 30 days after receiving an application under this subsection. The court may grant one or more extensions of not more than 30 days, if the court determines that additional time is needed. Any electronic surveillance subsequent to the court's action shall be conducted only if approved in accordance with section 105B. If the application is disapproved, the data collected may be used or disclosed only as authorized by the court.

''(c) SPECIFIC PERSONS AND PLACES NOT REQUIRED.—A certification under subsection (a) is not required to identify:

''(1) the person or foreign power against whom the electronic surveillance will be directed; or

"(2) the specific facilities, places, premises, or property at which the electronic surveillance will be directed or conducted.

"(d) DIRECTIVE.—With respect to an authorization of electronic surveillance under this section, the Attorney General, in consultation with the Director of National Intelligence, may direct a specified communications service provider, custodian, or other specified person, to: (1) furnish the applicant forthwith with all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in a manner that will protect the secrecy of the electronic surveillance and produce a minimum of interference with the services that provider, custodian, or other person is providing; and (2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the electronic surveillance or the aid furnished that such person wishes to maintain.

"(e) FAILURE TO COMPLY.—In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General, in consultation with the Director of National Intelligence, may invoke the aid of the court established under section 103(a) to compel compliance with the directive, and the court shall issue an order requiring the person to comply with the directive unless the court finds that the directive does not meet the requirements of this section or is otherwise unlawful. 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.

"(f) PENDENCY OF APPEAL. With the approval of a court of competent jurisdiction, the Government may continue any electronic surveillance affected by a

directive issued under this section during the pendency of consideration of an application submitted under section 105B, and any appeal process, including the period during which a petition for writ of certiorari may be pending and the period of any review by the Supreme Court of the United States.

"REPORT TO CONGRESS

SEC. 105D REPORT TO CONGRESS- Not later than four months after the date of the enactment of this Act, the Inspector General of the Department of Justice, in coordination with the Inspector General of the Office of the Director of National Intelligence and the Inspector General of the National Security Agency, shall inform, in a manner consistent with the national security, the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning electronic surveillance under this section during the previous four-month period. Among the elements of each report made under this section shall be–

(a) an assessment of whether the Act is functioning as intended and the degree to which the program is resulting in the collection of communications that originate or terminate inside the United States;

(b) a description of the incidents of non-compliance with a directive issued by the Attorney General under section 105C;

(c) a copy of any guidelines and procedures implementing this Act, including the guidelines established pursuant to section 105B(d);

(d) a description of any incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures established for determining that the electronic surveillance authorized by the Attorney General and Director of National Intelligence directed at persons reasonably believed to be outside the United States;

(e) a description of any incidents of non-compliance with respect to minimization procedures and approval requirements concerning U.S. persons; and

(f) the number of certifications and directives issued under section 105C during the reporting period.

(b) TECHNICAL AND CONFORMING AMENDMENT.—

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 105 the following:

"Sec. 105A. Clarification of surveillance of persons outside the United States.

"Sec. 105B. Additional procedure for court approval authorizing certain electronic surveillance.

"Sec. 105C. Immediate authorization of certain electronic surveillance.

"Sec. 105D. Report to Congress

SEC. 3. EFFECTIVE DATE; TRANSITION PROCEDURES

(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)) shall 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 Government also may file new applications, and the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) shall enter orders granting such applications pursuant to such Act, as long as the application meets the requirements set forth under the provisions of such Act as in effect on the day before the effective date of this Act. At the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)), shall extinguish any extant authorization to conduct electronic surveillance or physical search entered pursuant to such Act. Any electronic surveillance or physical search conducted pursuant to an order entered under this subsection shall be subject to the provisions of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in effect on the day before the effective date of this Act.

SEC. 4. SUNSET.–

(a) Except as provided in subsections (b) and (c) the amendments made by this Act shall cease to have force or effect 180 days after the date of enactment of this Act.

(b) Any order under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by this Act, in effect on the date described in paragraph (1) shall continue in effect until the date of the expiration of such order.

(c) The expiration of amendments pursuant to subsection (a) shall not have any effect upon the liability of any party under subsection (e) of section 105B. Notwithstanding subsection (a), subsection (e) of section 105B shall remain in effect with regard to action taken in accordance with sections 105A, B, C, and D.

** SENATE ARMED SERVICES COMMITTEE **

Fax Cover Sheet

Return this receipt to:

FAX TO:

Honorable J. M. McConnell
Director of National Intelligence

COMMENTS:

Response to letter from DNI addressed to Senator Carl Levin

FROM: _David Collins_____
Committee on Armed Services
United States Senate
Room SR-228, Russell Senate Office Building
Washington, D.C. 20510-6050

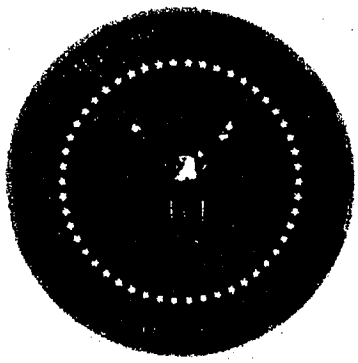
PHONE: (202) 224 - 1087

This transmission consists of _15_ pages, including this cover sheet.

House Permanent Select Committee on Intelligence

Hearing on the
Protect America Act 0f 2007

September 20, 2007



Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

STATEMENT FOR THE RECORD OF
J.MICHAEL McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES

September 20, 2007

Good morning Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee:

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector. I am pleased to be joined here today by Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and am sensitive to the fact, that FISA and the Protect America Act and the types of activities these laws govern, are of significant interest to Congress and to the public. For that reason, I will be as open as I can, but such discussion comes with degrees of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities. Therefore, on certain specific issues, I am happy to discuss matters further with Members in a classified setting.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, 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 or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented

Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. 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 international 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.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications,

certain "in wire" or fiber optic cable transmissions fell 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."

Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed 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.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts

to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. 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, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is <u>not</u> what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and

- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

Common Misperceptions About the Protect America Act

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only "foreign-to-foreign" communications from FISA's scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators

have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is who the target is, and where the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General

Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to this Committee and the Senate Intelligence Committee regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of the Senate and House Judiciary Committees, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of this Committee requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed staff members of this Committee regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four staff members of this Committee for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from this Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from the Senate Intelligence Committee and two staff members from the Senate Judiciary Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ's National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from this Committee, and the Senate Intelligence, Judiciary and Armed Services Committees regarding the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on this Committee and four of that Committee's staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four staff members of this Committee and this Committee's Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House

Judiciary Committee staff member. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

Additional Member and staff briefings are scheduled to take place this week.

Lasting FISA Modernization

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

Making the Changes Made by the Protect America Act Permanent

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed, however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will 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. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

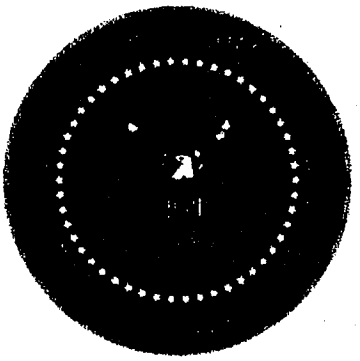
These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

Senate Select Committee on Intelligence

Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act

20 September 2007



Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

STATEMENT FOR THE RECORD OF
J.MICHAEL McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
SENATE SELECT COMMITTEE ON INTELLIGENCE

September 20, 2007

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

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector. I am pleased to be joined here today by National Security Agency Director, Lieutenant General Keith Alexander; Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division; and Federal Bureau of Investigation Deputy Director John Pistole.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, 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 or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's

members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. 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 international 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.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain "in wire" or fiber optic cable transmissions fell 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."

Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed 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.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated

among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and

improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. 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, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and
- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

Common Misperceptions About the Protect America Act

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only "foreign-to-foreign" communications from FISA's scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to

demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is who the target is, and where the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance

is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first

onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to this Committee and the House Intelligence Committee regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along

with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of the Senate and House Judiciary Committees, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of the House Intelligence Committee requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed staff members of this Committee regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four staff members of the House Intelligence Committee for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from the House Intelligence Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from this Committee and two staff members from the Senate Judiciary Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition,

representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ's National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of this Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from this Committee, and the House Intelligence, Judiciary and Armed Services Committees regarding the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on the House Intelligence Committee and four staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four staff members of the House Intelligence Committee and it's Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House Judiciary Committee staff members. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

Additional Member and staff briefings are scheduled to take place this week.

Lasting FISA Modernization

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

<u>Making the Changes Made by the Protect America Act Permanent</u>

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed, however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized

surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will 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. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

SSCI #2007-1498-A

April 9, 2007

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

Dear Director McConnell:

The Senate Select Committee on Intelligence intends to conduct a hearing on legislation to amend the Foreign Intelligence Surveillance Act to address present and future intelligence challenges on Tuesday, April 17, 2007. The open part of the hearing will take place in Room SDG-50 of the Dirksen Senate Office Building, at 2:30 p.m. After completing that part, the Committee will conduct the remainder of the hearing in closed session in Room SH-219.

The Committee requests that you and, if you wish, a senior representative of your office appear with the Director of the National Security Agency and a senior representative of the Department of Justice to discuss any legislation submitted in advance of the hearing intended to meet intelligence challenges under the Foreign Intelligence Surveillance Act. The testimony should address the implications of the legislation for our national security, the Constitution, and American values.

We understand that a consolidated written statement will be submitted on behalf of the Attorney General, the Director of the National Security Agency, and you. An electronic copy and paper copies of an unclassified statement for the record should be submitted to the Committee no later than noon on Monday, April 16, 2007. A separate classified statement for the record should also be submitted at that time. At the open session, we ask

that there be an approximately twenty-minute oral summary of the unclassified written testimony.

If your staff has any questions or would like to discuss this hearing further, please have them contact Ms. Christine Healey, of the Committee staff, at (202) 224-1700.

Sincerely,

John D. Rockefeller IV
Chairman

Christopher S. Bond
Vice Chairman

cc: The Honorable Alberto Gonzales
General Keith B. Alexander

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

September 11, 2007

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

Dear Director McConnell:

At the hearing held in our Committee last week, a number of serious concerns were raised by several members about your recent interview with the El Paso Times, in which you revealed "previously classified details of government surveillance" activities. K. Shrader, "Spy chief reveals classified details about surveillance."[1] Especially in light of the Administration's previous refusal to provide such information to Congress, this selective disclosure of information raises troubling questions that we ask you to address prior to your scheduled appearance before the Committee next week to discuss proposed changes to the Foreign Intelligence Surveillance Act (FISA).[2]

Previously, when the Judiciary Committee has attempted to obtain this and similar information about Administration surveillance programs, the response has been that information about surveillance programs is "classified and sensitive, and therefore cannot be discussed" in

---

[1] El Paso Times (Aug. 22, 2007).

[2] According to the transcript of your El Paso interview, posted online at http://www.elpasotimes.com/news/ci_6685679, you claimed that the recently-enacted short-term FISA revisions were needed to deal with a backlog caused by resources needed to prepare applications for FISA warrants, asserting that hundreds of man-hours were needed to obtain each warrant. You discussed the number of Americans whose communications have been targeted for direct interception as "100 or less", apparently in an attempt to rebut the concern that significant numbers of U.S. persons' communications would be caught in a dragnet under the new law, although the number of Americans targeted (as opposed to the number overheard) does not address that concern. You discussed the mechanics of FISA applications and court review, including changes in FISC caselaw since the beginning of 2007. You confirmed that "private sector" telecommunications companies "assisted" in warrantless government surveillance in arguing for retroactive immunity for such companies. You also suggested that the public and Congressional reporting and debate over FISA and intelligence-gathering methods "means that some Americans are going to die."

responding to Committee questions.[3] In a public affidavit submitted earlier this year as part of In *re National Security Agency Telecommunications Records Litigation*,[4] moreover, you asserted the state secrets doctrine to seek dismissal of a case concerning foreign intelligence surveillance, attempting to prevent even confirmation as to whether U.S. companies were involved in surveillance activities. During the very week you disclosed the involvement of private companies in your El Paso interview, the Justice Department continued to make that argument before the Ninth Circuit Court of Appeals.[5]

In light of these concerns, we ask that you answer the following questions in writing prior to your testimony next week::

1. Was a specific decision made to declassify any previously-classified information contained in the El Paso Times interview and, if so, when, by whom, and under what authority? Please provide the background and a specific explanation for any such decision.

2 In light of your public confirmation of the involvement of "private sector" telecommunications companies in the Administration's surveillance programs, what is the specific justification for your claim a few months earlier in litigation that confirmation of such involvement cannot be permitted under the state secrets doctrine? What steps have been or will be taken by you or by the Justice Department with respect to the earlier assertions, now contradicted by the El Paso Times interview, that participation of private companies in Administration surveillance programs cannot be confirmed?

3. The Administration's report to Congress states that 2,181 FISA applications were filed in 2006. If each application takes 200 man-hours, as you suggested in the El Paso interview, this would require at least 218 attorneys and analysts working full-time for more than 436,000 hours on nothing but warrant applications. Do you continue to stand by your assertion to the El Paso Times that "[i]t takes about 200 hours" to do the application for each phone number?

4. According to an article in today's New York Times, you made another selective disclosure of classified information when you claimed yesterday to a Senate committee in public session that the temporary FISA law just passed by Congress

---

[3] See, e.g., Letter of Assistant Attorney General William Moschella in response to Judiciary Committee questions concerning the Terrorist Surveillance Program (March 24, 2006); Letter of Principal Deputy Assistant Attorney General Richard Hertling in response to Judiciary Committee questions concerning Foreign Intelligence Surveillance Act and Court Orders (June 21, 2007).

[4] MDL Dkt. No. 06-1791-VRW (ND CA 2007).

[5] See, e.g., Washington Post, "Judges Skeptical of State-Secrets Claim" (August 16, 2007).

helped lead to the arrests last week of three Islamic militants accused of planning bomb attacks in Germany. The article also states, however, that another official stated that you may have misspoken and that the intercepts in question were obtained under the old law.[6] Please state whether a specific decision was made to de-classify the information you provided to the Senate Committee and, if so, when, by whom, under what authority, and what was the specific background and explanation. In addition, please clarify whether the intercepts in question were foreign-to-foreign, as your statement implied, and whether they were in fact obtained under the old FISA law or the new FISA law.

We look forward to your prompt reply to these questions and to your continued cooperation as Congress considers FISA's future. Responses and questions should be directed to the Judiciary Committee office, 2138 Rayburn House Office Building, Washington, D.C. 20515 (tel: 202-225-3951; fax: 202-225-7680). It would be of the utmost assistance to the Committee if your responses to the above questions were provided to us by no later than 2 PM on Monday, September 17, 2004, in advance of your testimony before us the following day. Thank you for your assistance.

Sincerely,

John Conyers, Jr.
Chairman

Jerrold Nadler
Chairman, Subcommittee on the Constitution, Civil Rights and Civil Liberties

Robert C. "Bobby" Scott
Chairman, Subcommittee on Crime, Terrorism and Homeland Security

cc: Hon. Lamar S. Smith
Hon. Trent Franks
Hon. J. Randy Forbes

[6] New York Times, "New U.S. Law Credited in Arrests Abroad" (Sept. 11, 2007)

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

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

MICHAEL J. DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

September 11, 2007

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

Dear Director McConnell:

At yesterday's hearing before the Senate Homeland Security and Government Affairs Committee, Senator Leiberman asked you whether the so-called Protect America Act, which President Bush signed into law on August 5, 2007, facilitated the detection of the German terrorist plot.

You responded, "Yes sir, it did."

This statement is at odds with information I have received. Specifically, I am told by senior American officials that U.S. assistance to German intelligence was based on collection under the Foreign Intelligence Surveillance Act (FISA), *several months* before its modification by Congress in August. Accordingly, the new law did *not* lead to the arrests of the three terrorist plotters, as you claimed.

While revising FISA may provide a tool that could enhance future operations, it was not in play in the Germany case. In fact, FISA, which you repeatedly claim is "outdated," was precisely the tool that helped disrupt this plot.

Members of Congress need accurate information from the Intelligence Community, and I am deeply concerned that your comments may be used improperly. I therefore urge you to issue a public statement immediately to confirm that the surveillance used to assist in the disruption of German plot was collected pursuant to FISA before the passage of the Protect America Act.

Sincerely,

Silvestre Reyes
Chairman

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

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

MICHAEL J. DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

September 11, 2007

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

Dear Director McConnell:

On Thursday, September 20, 2007, the House Permanent Select Committee on Intelligence will hold a hearing on the Foreign Intelligence Surveillance Act (FISA) and authorities for the National Security Agency (NSA) surveillance activities. The hearing will take place from 10:00 am until 1:00 pm. We will notify you as to the location once a hearing room has been designated. We cordially invite you to testify in this hearing that will begin as an open session and then move to a closed session.

On August 4, 2007, Congress passed legislation to adopt a temporary revision of FISA. The Committee seeks to understand the impact of these changes on the civil liberties of American citizens and the need for permanent modification to FISA. This hearing is one in a series of hearings the Committee will convene in the coming weeks to assess the future of FISA.

In preparing your testimony, please consider the following issues: (1) the legal authorities given to the NSA after September 11, 2001, to include the way in which the NSA operated under those authorities; (2) the legal authorities NSA operated under beginning in January 2007, after the President brought the publicly described "Terrorist Surveillance Program" to the Foreign Intelligence Surveillance Court, to include the way in which those authorities have evolved; (3) how NSA will operate under the legal authorities passed by Congress on August 4, 2007; (4) the impact the temporary changes have had on intelligence collection; (5) the question of retrospective liability for private sector entities that may have assisted the U.S. government in conducting surveillance after September 11, 2001; and (6) any permanent changes Congress should consider making to FISA when the temporary authorities expire.

Please provide your statement for the record by close of business on September 17, 2007 along with the names of any supporting attendees. Please limit your oral testimony to five minutes.

Questions regarding this hearing may be directed to Ms. Wyndee Parker, Deputy Staff Director and General Counsel, at 202-225-7690.

Sincerely,

Silvestre Reyes
Chairman

Peter Hoekstra
Ranking Member

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

September 12, 2007

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

Dear Mr. McConnell:

The House Committee on the Judiciary will hold a hearing on Tuesday, September 18, 2007, at 11:00 a.m. in room 2141 Rayburn House Office Building. The hearing is on Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights.

I would like to invite you to testify at this hearing. Please prepare a written statement for submission to the Committee prior to your appearance. The written statement may be as extensive as you wish and will be included in the hearing record. To allow sufficient time for questions at the hearing, please briefly highlight the most significant points of the written statement in an oral presentation lasting five minutes or less. Oral testimony at the hearing, including answers to questions, will be printed as part of the verbatim record of the hearing. Only transcription errors may be edited subsequent to the hearing.

To facilitate preparation for the hearing, please send an electronic copy of your written statement and curriculum vitae to the Committee 48 hours in advance of the hearing. The Committee will publish the statement on our website and, therefore, requests that you provide the documents in Word Perfect, Microsoft Word, or Adobe Acrobat. Please number all pages of the written statement, and attach a cover page with your name, position, date, and the title of the hearing. These documents may be e-mailed to Lou DeBaca on my staff at Lou.DeBaca@mail.house.gov.

In addition, the Committee requests that you provide 50 copies of your written statement to Lou DeBaca, 2138 Rayburn House Office Building, Washington, DC, 20515, 48 hours in advance of the hearing. Due to delays with our current mail delivery system, the copies should be hand delivered in an unsealed package. If this is not possible, please bring the copies with you the day of the hearing. Should you intend to introduce a published document or report as part of your written statement, I ask that you provide 60 copies for the hearing. Should such material be available on the Internet, please prepare a page containing citations to such material and provide the Committee with 50 copies.

If you have any questions or concerns, please contact Lou DeBaca on my staff at 202-225-3951.

I look forward to your participation in the hearing.

Sincerely,

John Conyers, Jr.
Chairman

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

FAX COVER SHEET

DATE: 9/13/07

TO: Mr. Mike McConnell

FAX NO.: [redacted]

FROM: Matthew Morgan Fax No.: (202) 225-7680

NUMBER OF PAGES IN THIS TRANSMISSION: 3 (including cover)

COMMENTS: Witness Invitation Letter

PLEASE CALL IF THERE ARE ANY PROBLEMS WITH THIS TRANSMISSION
(202) 225-3951

UNCLASSIFIED

THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

April 12, 2007

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

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

Dear Mr. Chairman and Ranking Member Hoekstra:

I am pleased to provide you with the Administration's proposal to modernize FISA (Title IV of the proposed Fiscal Year 2008 Intelligence Authorization Act) in advance of the hearing on legislation to amend the Foreign Intelligence Surveillance Act (FISA) to be conducted by the Senate Select Committee on Intelligence (SSCI) on April 17, 2007. Since 1978, FISA has served as an important framework governing Intelligence Community activities, but dramatic changes in technology have created unanticipated consequences for the FISA system. I believe this proposed legislation will restore FISA to its original purpose and significantly improve the intelligence efforts to protect America.

The proposal seeks to accomplish several goals. First, it brings FISA up to date with the changes in communications technology and makes the statute technology-neutral. It preserves the privacy protections built in to the original FISA statute. Most importantly, it ensures that the privacy interests of persons in the United States are protected. It enhances the authority to secure assistance from private entities, and makes certain they are protected from liability for having assisted the government in its counterterrorism efforts. Finally, it makes changes that will streamline the FISA process so that the Intelligence Community can effectively direct resources and ensure that the rights and safety of all Americans are protected.

The proposed legislation resulted from an extensive interagency effort that began over a year ago and included both participants from inside and outside the Intelligence Community. We have briefed and discussed various proposals with staff of both the SSCI and the Permanent Select Committee on Intelligence of the House of Representatives (HPSCI) and provided them with numerous briefings on the topic. In addition, congressional committees held numerous hearings related to this topic in 2006.

The enclosed document constitutes the Administration's proposal for FISA modernization in its entirety. The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presenting of these legislative proposals for your consideration and the consideration of Congress at this time.

The remainder of our proposed Fiscal Year 2008 Intelligence Authorization Act, not included in this transmission, contains provisions unrelated to FISA modernization, but of interest to the Intelligence Community. These unrelated provisions will be formally transmitted to you shortly (Titles I, II, and III of the proposed Fiscal Year 2008 Intelligence Authorization Act).

I look forward to working with the Congress to ensure the enactment of this critical legislation. 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

Enclosure as stated

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

September 20, 2007

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

Dear Director McConnell:

Thank you for agreeing to appear and testify at the Senate Committee on the Judiciary hearing entitled "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?" scheduled for September 25, 2007, at 9:30 a.m. in room 216 of the Hart Senate Office Building. I look forward to hearing your testimony, and to working with you on this important issue.

Committee rules require that that your written testimony be provided 48 hours in advance of the hearing. Please provide 75 hard copies of the written testimony and your curriculum vitae by that time. Send the hard copies as soon as possible to the attention of Jennifer Price, Hearing Clerk, Senate Committee on the Judiciary, 224 Dirksen Senate Office Building, Washington, D.C. 20510. Please also send electronic copy of the testimony and a short biography via email to Jennifer_Price@judiciary-dem.senate.gov.

Sincerely,

Patrick Leahy

PATRICK LEAHY
Chairman

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

Facsimile Cover Sheet

Please Deliver to: Hon. Michael McConnell

Fax No. [redacted]

From: Chairman Patrick Leahy

Phone: 202-224-9376

Number of Pages Including Cover: 2

Comments:

If there are any problems with this transmission, please call: 224-9376

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

STATEMENT FOR THE RECORD OF
J.M. McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
JUDICIARY COMMITTEE
HOUSE OF REPRESENTATIVES

September 18, 2007

Good morning Chairman Conyers, Ranking Member Smith, and Members of the Committee.

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector. I am pleased to be joined here today by my General Counsel, Ben Powell, and Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and am sensitive to the fact, that FISA and the Protect America Act and the types of activities these laws govern, are of significant interest to Congress and to the public. For that reason, I will be as open as I can, but such discussion comes with degrees of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities. Therefore, on certain specific issues, I am happy to discuss matters further with Members in a classified setting.

I have not appeared before this Committee previously as a witness, and so I would like to take a moment to introduce myself to you. I am a career intelligence professional. I spent the majority of my career as a Naval

Intelligence Officer. During the periods of Desert Shield and Desert Storm, as well as during the dissolution of the Soviet Union, I served as the primary Intelligence Officer for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense. I then had the privilege of serving as the Director of the National Security Agency (NSA) from 1992 to 1996, under President Clinton. In 1996, I retired from the U.S. Navy after 29 years of service - 26 of those years spent as a career Intelligence Officer. I then turned to the private sector as a consultant, where for ten years I worked to help the government achieve better results on a number of matters, including those concerning intelligence and national security. I have been in my current capacity as the nation's second Director of National Intelligence (DNI) since February 2007.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, 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 or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on

both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. 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 international 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.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain "in wire" or fiber optic cable transmissions fell 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."

Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed 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.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider

attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. 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, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person

reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign

intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and
- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

Common Misperceptions About the Protect America Act

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only "foreign-to-foreign" communications from FISA's scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is who the target is, and where the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct

electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to the House and Senate Intelligence Committees regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of this Committee and the Senate Judiciary Committee, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of the House Permanent Select Committee on Intelligence requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed House Intelligence Committee staff members regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four House Intelligence Committee staff members for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from the House Intelligence Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from the Senate Intelligence Committee and two staff members from the Senate Judiciary Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ's National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from the House Intelligence Committee, and the Senate Intelligence, Judiciary and Armed Services Committees regarding

the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on the House Intelligence Committee and four of that Committee's staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four House Intelligence Committee staff members and the Committee's Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House Judiciary Committee staff member. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

Additional Member and staff briefings are scheduled to take place this week.

Lasting FISA Modernization

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

Making the Changes Made by the Protect America Act Permanent

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do

a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed, however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will 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. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

UNCLASSIFIED

THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

April 12, 2007

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

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman and Vice Chairman Bond:

I am pleased to provide you with the Administration's proposal to modernize FISA (Title IV of the proposed Fiscal Year 2008 Intelligence Authorization Act) in advance of the hearing on legislation to amend the Foreign Intelligence Surveillance Act (FISA) to be conducted by the Senate Select Committee on Intelligence (SSCI) on April 17, 2007. Since 1978, FISA has served as an important framework governing Intelligence Community activities, but dramatic changes in technology have created unanticipated consequences for the FISA system. I believe this proposed legislation will restore FISA to its original purpose and significantly improve the intelligence efforts to protect America.

The proposal seeks to accomplish several goals. First, it brings FISA up to date with the changes in communications technology and makes the statute technology-neutral. It preserves the privacy protections built in to the original FISA statute. Most importantly, it ensures that the privacy interests of persons in the United States are protected. It enhances the authority to secure assistance from private entities, and makes certain they are protected from liability for having assisted the government in its counterterrorism efforts. Finally, it makes changes that will streamline the FISA process so that the Intelligence Community can effectively direct resources and ensure that the rights and safety of all Americans are protected.

The proposed legislation resulted from an extensive interagency effort that began over a year ago and included both participants from inside and outside the Intelligence Community. We have briefed and discussed various proposals with staff of both the SSCI and the Permanent Select Committee on Intelligence of the House of Representatives (HPSCI) and provided them with numerous briefings on the topic. In addition, congressional committees held numerous hearings related to this topic in 2006.

The enclosed document constitutes the Administration's proposal for FISA modernization in its entirety. The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presenting of these legislative proposals for your consideration and the consideration of Congress at this time.

The remainder of our proposed Fiscal Year 2008 Intelligence Authorization Act, not included in this transmission, contains provisions unrelated to FISA modernization, but of interest to the Intelligence Community. These unrelated provisions will be formally transmitted to you shortly (Titles I, II, and III of the proposed Fiscal Year 2008 Intelligence Authorization Act).

I look forward to working with the Congress to ensure the enactment of this critical legislation. 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

Enclosure as stated

FISA MODERNIZATION PROVISIONS OF THE PROPOSED FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION

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 (1) of such section is amended by striking subsection (1).

(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.

FISA MODERNIZATION PROVISIONS OF THE PROPOSED FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION

SECTIONAL ANALYSIS

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.