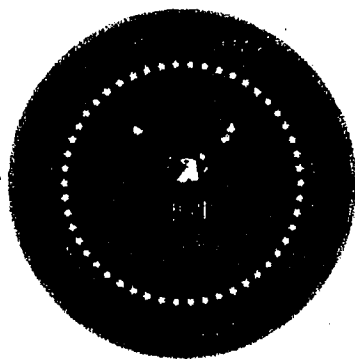


**Senate Select Committee on Intelligence**

**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](http://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 its 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.

### **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.

JOHN D. ROCKEFELLER IV, WEST VIRGINIA, CHAIRMAN  
CHRISTOPHER S. BOND, MISSOURI, VICE CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA  
RON WYDEN, OREGON  
EVAN BAYH, INDIANA  
BARBARA A. MIKULSKI, MARYLAND  
RUSSELL D. FEINOLD, WISCONSIN  
BILL NELSON, FLORIDA  
SHELDON WHITEHOUSE, RHODE ISLAND

JOHN WARNER, VIRGINIA  
CHUCK HAGEL, NEBRASKA  
SANDY CHAMBLISS, GEORGIA  
ORIN HATCH, UTAH  
OLYMPIA J. SNOWE, MAINE  
RICHARD BURR, NORTH CAROLINA

## United States Senate

SELECT COMMITTEE ON INTELLIGENCE  
WASHINGTON, DC 20510-6471

SSCI #2007-1498-A

HARRY REID, NEVADA, EX OFFICIO  
MATT MCCONNELL, KENTUCKY, EX OFFICIO  
CARL LEVIN, MICHIGAN, EX OFFICIO  
JOHN MACAIN, ARIZONA, EX OFFICIO

ANDREW W. JOHNSON, STAFF DIRECTOR  
LOUIS B. TUCKER, MINORITY STAFF DIRECTOR  
KATHLEEN P. MCGHEE, CHIEF CLERK

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.

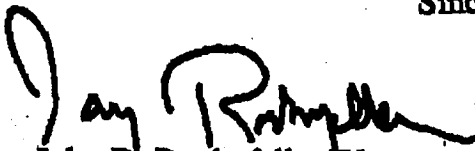
We understand that a consolidated written statement will be submitted on behalf of the Attorney General, the Director of the National Security Agency, and you. An electronic copy and paper copies of an unclassified statement for the record should be submitted to the Committee no later than noon on Monday,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

The Honorable J.M. McConnell  
April 9, 2007  
Page Two

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

JOHN CONYERS, JR., Michigan  
CHAIRMAN

HOWARD L. BERMAN, California  
RICK BOUCHER, Virginia  
JERROLD NADLER, New York  
ROBERT C. "BOBBY" SCOTT, Virginia  
MELVIN L. WATT, North Carolina  
ZOE LOPKIN, California  
SHERA JACKSON LEE, Texas  
MAGNIE WATERS, California  
WILLIAM D. DELAHUNT, Massachusetts  
ROBERT WEXLER, Florida  
LINDA T. SANDOZ, California  
STEVE COHEN, Tennessee  
HENRY C. "HANK" JOHNSON, JR., Georgia  
BETTY SUTTON, Ohio  
LUIS V. GUTIERREZ, Illinois  
BRAD SHERMAN, California  
TAMMY BALDWIN, Wisconsin  
ANTHONY D. WEINER, New York  
ADAM B. SCHIFF, California  
ARTHUR DAVIS, Alabama  
DEBBIE WASSERMAN SCHULTZ, Florida  
KEITH ELLISON, Minnesota

LAMAR L. SMITH, Texas  
RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin  
HOWARD COBLE, North Carolina  
ELTON GALLEGLY, California  
BOB GOODLATTE, Virginia  
STEVE CHABOT, Ohio  
DANIEL E. LUNGREN, California  
CHRIS CANNON, Utah  
RIC KELLER, Florida  
DANIEL E. ROSS, California  
MIKE PENCE, Indiana  
J. RANDY FORBES, Virginia  
STEVE KING, Iowa  
TOM FEENEY, Florida  
TRENT FRANKS, Arizona  
LOUIE GOMMERT, Texas  
JIM JORDAN, Ohio

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."<sup>1</sup> 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).<sup>2</sup>

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

<sup>1</sup> El Paso Times (Aug. 22, 2007).

<sup>2</sup> According to the transcript of your El Paso interview, posted online at [http://www.elpasotimes.com/news/cj\\_6685679](http://www.elpasotimes.com/news/cj_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."

The Honorable Michael "Mike" McConnell  
Page Two

responding to Committee questions.<sup>3</sup> In a public affidavit submitted earlier this year as part of *In re National Security Agency Telecommunications Records Litigation*,<sup>4</sup> 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.<sup>5</sup>

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

---

<sup>3</sup>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).

<sup>4</sup>MDL Dkt. No. 06-1791-VRW (ND CA 2007).

<sup>5</sup>See, e.g., Washington Post, "Judges Skeptical of State-Secrets Claim" (August 16, 2007).

The Honorable Michael "Mike" McConnell  
Page Three

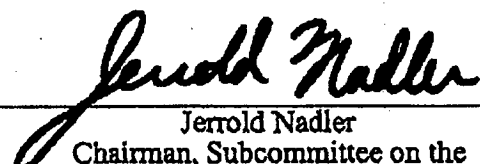
helped lead to the arrests last week of three Islamic militants accused of planning bomb attacks in Germany. The article also states, however, that another official stated that you may have misspoken and that the intercepts in question were obtained under the old law.<sup>6</sup> Please state whether 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.

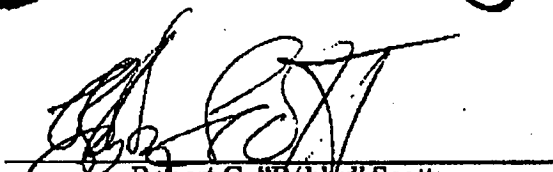
Sincerely,



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

---

<sup>6</sup>New York Times, "New U.S. Law Credited in Arrests Abroad" (Sept. 11, 2007)

SILVESTRE REYES, TEXAS, CHAIRMAN

ALCEE L. HASTINGS, FLORIDA, VICE-CHAIRMAN  
LEONARD L. BOSWELL, IOWA  
ROBERT E. (BOB) CRAMER, JR., ALABAMA  
ANNA G. ESHOO, CALIFORNIA  
RICHARD W. HOLT, NEW JERSEY  
C.A. DUTCH RUPPERSBERGER, MARYLAND  
JOHN F. TIERNEY, MASSACHUSETTS  
MIKE THOMPSON, CALIFORNIA  
JANICE D. SCHAKOWSKY, ILLINOIS  
JAMES R. LANGRISH, RHODE ISLAND  
PATRICK J. MURPHY, PENNSYLVANIA

PETER HOSKSTADT, MICHIGAN, RANKING MEMBER  
TERRY EVERETT, ALABAMA  
ELTON GALLEGLY, CALIFORNIA  
HEATHER WILSON, NEW MEXICO  
MAC THORNBERRY, TEXAS  
JOHN M. MCNUGH, NEW YORK  
TODD TANKY, KANSAS  
MIKE ROGERS, MICHIGAN  
DARRELL E. ISSA, CALIFORNIA

NANCY PELOSI, SPEAKER  
JOHN A. BOEHNER, REPUBLICAN LEADER

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

H-405, THE CAPITOL  
WASHINGTON, DC 20515  
(202) 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 Lieberman 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.

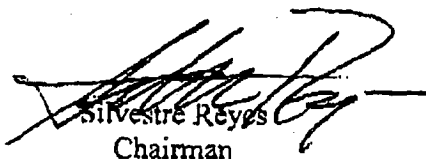
You responded, "Yes sir, it did."

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



SILVESTRE REYES, TEXAS, CHAIRMAN

ALCEE L. HASTINGS, FLORIDA, VICE-CHAIRMAN

LEONARD L. BODWELL, IOWA

ROBERT E. (BUD) CRAMER, JR., ALABAMA

ANNA E. ESHOO, CALIFORNIA

RUDEN D. HOLT, NEW JERSEY

C.A. DUTCH RUPPERSBERGER, MARYLAND

JOHN P. TIERNEY, MASSACHUSETTS

MIKE THOMPSON, CALIFORNIA

JANICE D. SCHAKOWSKY, ILLINOIS

JAMES R. LANGEVIN, RHODE ISLAND

PATRICK J. MURPHY, PENNSYLVANIA

PETER MOEKSTRA, MICHIGAN, RANKING MEMBER

TERRY EVERETT, ALABAMA

ELTON GALLEGLY, CALIFORNIA

HEATHER WILSON, NEW MEXICO

MAC THORNBERRY, TEXAS

JOHN M. MCNUGH, NEW YORK

TODD TIAHT, KANSAS

MIKE ROGERS, MICHIGAN

DARRELL E. ISSA, CALIFORNIA

NANCY PELOSI, SPEAKER

JOHN A. BOEHNER, REPUBLICAN LEADER

## U.S. HOUSE OF REPRESENTATIVES

### PERMANENT SELECT COMMITTEE ON INTELLIGENCE

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

MICHAEL J. DELANEY

STAFF DIRECTOR

MICHAEL MEERMAN'S  
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

JOHN CONYERS, JR., Michigan  
CHAIRMAN

HOWARD L. Berman, California  
RICK BOUCHER, Virginia  
JERROLD NADLER, New York  
ROBERT C. "BOBBY" SCOTT, Virginia  
MELVIN L. WATT, North Carolina  
ZOE LOPKIN, California  
SHERA JACKSON LEE, Texas  
MAZONI WATERS, California  
WILLIAM D. DELAHUNT, Massachusetts  
ROBERT WEXLER, Florida  
LINDA T. SANCHEZ, California  
STEVE COHEN, Tennessee  
HENRY C. "HANK" JOHNSON, JR., Georgia  
BETTY BUTTON, Ohio  
LUIS V. GUTIERREZ, Illinois  
GRAD SHENMAN, California  
TAMMY BALDWIN, Wisconsin  
ANTHONY D. WEINER, New York  
ADAM S. SCHIFF, California  
ARTHUR DAVIS, Alabama  
DORRIS WASSERMAN SCHULTZ, Florida  
KEITH CLUBB, Minnesota

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

LAMAR S. SMITH, Texas  
RANKING MINORITY MEMBER

F. JAMES SENESENRENNER, JR., Wisconsin  
HOWARD COBLE, North Carolina  
ELTON GALLEGLY, California  
BOB GOODLATTE, Virginia  
STEVE CHABOT, Ohio  
DANIEL E. LUNGREN, California  
CHRIS CANNON, Utah  
RIC KLEUR, Florida  
DANIEL L. ISSA, California  
MIKE PENCE, Indiana  
J. RANDY FORBES, Virginia  
STEVE KING, Iowa  
TOM FREEMAN, Florida  
TRENT FRANKS, Arizona  
LOUIE GOMMERT, Texas  
JIM JORDAN, Ohio

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](mailto:Lou.DeBaca@mail.house.gov).

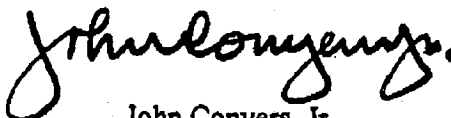
Mr. Mike McConnell  
Page Two  
September 12, 2007

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

JOHN CONYERS, JR., Michigan  
CHAIRMAN

HOWARD L. Berman, California  
RICK BOUCHER, Virginia  
JERROLD HADLER, New York  
ROBERT C. "BOBBY" SCOTT, Virginia  
MELVIN L. WATT, North Carolina  
ZOE LOPRESTI, California  
BRIAN JACOBSON, Tennessee  
MARTINE WATERS, California  
WILLIAM D. DELAHUNT, Massachusetts  
ROBERT WEXLER, Florida  
LINDA T. SANCHEZ, California  
STEVE COHEN, Tennessee  
HENRY C. "HANK" JOHNSON, JR., Georgia  
BETTY BUTTON, Ohio  
LUS V. GUTIERREZ, Illinois  
BRAD EDERMAN, California  
TAMMY BALDWIN, Wisconsin  
ANTHONY D. WEINER, New York  
ADAM S. SCHIFF, California  
ARTUR DAVIS, Alabama  
DEBBIE WASSERMAN SCHULTZ, Florida  
KEITH CLISON, Minnesota

ONE HUNDRED TENTH CONGRESS

# Congress of the United States

## House of Representatives

### COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6218

(202) 225-3951

<http://www.house.gov/judiciary>

### FAX COVER SHEET

LAMAR S. SMITH, Texas  
RANKING MEMBER

F. JAMES SCHENCKENBERGER, JR., Wisconsin  
HOWARD COBLE, North Carolina  
ELTON GALLEGLY, California  
BOB GOODLATTE, Virginia  
STEVE CHABOT, Ohio  
DANIEL E. LUNYON, California  
CHRIS CANNON, Utah  
RICK KELLER, Florida  
DARNELL E. ISEA, California  
MIKE PENCE, Indiana  
J. RALPH FORD, Virginia  
STEVE KING, Iowa  
TOM HENRY, Florida  
TRENT FRANKS, Arizona  
LOUIE GOMMERT, Texas  
JIM JORDAN, Ohio

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.

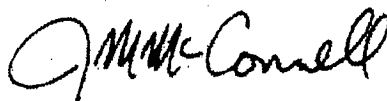
The proposed legislation resulted from an extensive interagency effort that began over a year ago and included both participants from inside and outside the Intelligence Community. We have briefed and discussed various proposals with staff of both the SSCI and the Permanent Select Committee on Intelligence 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,

A handwritten signature in black ink, appearing to read "J.M. McConnell". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

J.M. McConnell

Enclosure as stated

UNCLASSIFIED

000154

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS  
JOSEPH R. BIDEN, JR., DELAWARE  
HERB KOHL, WISCONSIN  
DIANNE FEINSTEIN, CALIFORNIA  
RUSSELL D. FEINGOLD, WISCONSIN  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
BENJAMIN L. CARDIN, MARYLAND  
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA  
ORRIN G. HATCH, UTAH  
CHARLES E. GRASSLEY, IOWA  
JON KYL, ARIZONA  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
SAM BROWNBACK, KANSAS  
TOM COBURN, OKLAHOMA

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*  
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

September 20, 2007

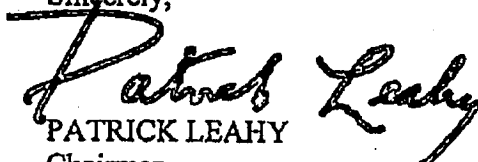
Hon. Michael McConnell  
Director of National Intelligence  
Office of the Director of National Intelligence  
Washington, DC 20511

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](mailto:Jennifer_Price@judiciary-dem.senate.gov).

Sincerely,

  
PATRICK LEAHY  
Chairman



COMMITTEE ON THE JUDICIARY  
WASHINGTON, DC 20510-6275

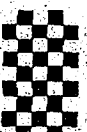
Please Deliver to: Hon. Michael McConnell

From: Chairman Patrick Leahy

Phone: 202-224-9376

**Comments:**

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](http://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 authorize 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,

A handwritten signature in dark ink, appearing to read "J.M. McConnell". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

J.M. McConnell

Enclosure as stated

UNCLASSIFIED

000176

**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.
- Sec. 401. Definitions.
- Sec. 402. Attorney General Authorization for Electronic Surveillance.
- Sec. 403. Jurisdiction of FISA Court.
- Sec. 404. Applications for Court Orders.
- Sec. 405. Issuance of an Order.
- Sec. 406. Use of Information.
- Sec. 407. Weapons of Mass Destruction.
- Sec. 408. Liability Defense.
- Sec. 409. Amendments for Physical Searches.
- Sec, 410. Amendments for Emergency Pen Registers and Trap and Trace Devices.
- Sec. 411. Mandatory Transfer for Review
- Sec. 412. Technical and Conforming Amendments.
- Sec. 413. Effective Date.
- Sec. 414. Construction; Severability.

**SEC. 400. SHORT TITLE**

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

**SEC. 401. DEFINITIONS.**

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

(1) in subparagraph (B), by striking ``; or'' and inserting ``;''; and

(2) by adding at the end the following:

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

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

``(f) 'Electronic surveillance' means—

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



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

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

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

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

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

(2) by striking subsection (4).

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

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

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

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

**“AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR  
FOREIGN INTELLIGENCE PURPOSES**

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

**“(1) certifies in writing under oath that—**

**“(A) the electronic surveillance is  
directed at—**

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

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

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

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

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

“(b) MINIMIZATION PROCEDURES.—An electronic surveillance authorized under this section may be conducted only in accordance with the Attorney General’s certification and the minimization procedures. The Attorney General shall assess compliance with such procedures and shall report such

assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under the provisions of section 108(a).

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

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

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

“AUTHORIZATION FOR ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION

“SEC. 102A. (a) IN GENERAL.—Notwithstanding any other law, the President, acting through the Attorney General may, for periods of up to one year, authorize

the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that the Attorney General has determined that-

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

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

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

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

“(b) SPECIFIC PLACE NOT REQUIRED.—A

certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

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

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

the House of Representatives and the Select Committee on Intelligence of the Senate under section 108(a).

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

``SEC. 102B. (a) DIRECTIVE.--With respect to an authorization of electronic surveillance under section 102 or an authorization of an acquisition under section 102A, the Attorney General may direct a person to--

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

``(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the electronic surveillance or acquisition or the aid furnished that such person wishes to maintain.

``(b) COMPENSATION.--The Government shall compensate, at the prevailing rate, a person for

providing information, facilities, or assistance pursuant to subsection (a).

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

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

“(B) The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges serving in the pool established by section 103(e) (1). Not later



than 24 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

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

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

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

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

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

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

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

“USE OF INFORMATION ACQUIRED UNDER SECTION 102A

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

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

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

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

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

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

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

“(A) the information was unlawfully acquired; or

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

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

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

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

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

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

“(f) SUPPRESSION OF EVIDENCE; DENIAL OF MOTION.—

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



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

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

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

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

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

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

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

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

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

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

foreign intelligence information.

"102C. Use of information acquired under section  
102A."

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

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

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

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

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

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

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

(1) in subsection (a)-

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

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

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

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

(i) in the matter preceding subparagraph

(A), by striking ``or officials designated'' and all that follows through ``consent of the Senate'' and inserting ``designated by the President to authorize electronic surveillance for foreign intelligence purposes'';

(ii) in subparagraph (C), by striking ``techniques;'' and inserting ``techniques; and'';

(iii) by striking subparagraph (D); and

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

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

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

(i) by striking ``a statement'' and inserting ``a summary statement''; and

(ii) by striking ``application;'' and inserting ``application; and''; and

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

(2) by striking subsection (b);

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

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

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

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

(1) in subsection (a)—

(A) by striking paragraph (1); and

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

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

(A) in subparagraph (D), by striking  
“surveillance;” and inserting “surveillance;  
and”;

(B) in subparagraph (E), by striking “approved;  
and” and inserting “approved.”; and

(C) by striking subparagraph (F).

(3) by striking subsection (d);

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

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

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

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

“(2) Extensions of an order issued under this title  
may be granted on the same basis as an original order

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

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

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

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

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

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

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



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

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

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

(4)–

(A) by striking ``a wire or'' and inserting

``an''; and

(B) by striking ``physical search'' and inserting

``physical search or in response to a

certification by the Attorney General or a

designee of the Attorney General seeking

information, facilities, or technical assistance

from such person under section 102B''; and

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

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

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

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

(1) in subsection (i)—

(A) by striking ``radio communication'' and inserting ``communication''; and

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

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

"(1) 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 (1) of such section (50 U.S.C. 1801(1)) is amended to read as follows:

''(1) '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 11<sup>th</sup> 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.