

Testimony of

# The Honorable J. Michael McConnell

September 25, 2007

STATEMENT FOR THE RECORD OF  
J.MICHAEL McCONNELL  
DIRECTOR OF NATIONAL INTELLIGENCE  
BEFORE THE  
JUDICIARY COMMITTEE  
UNITED STATES SENATE  
September 25, 2007

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

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

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

I have not appeared before this Committee previously as a witness, and so I would like to take a moment to introduce myself to you. I am a career intelligence professional. I spent the majority of my career as a Naval Intelligence Officer. During the periods of Desert Shield and Desert Storm, as well as during the dissolution of the Soviet Union, I served as the primary Intelligence Officer for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense. I then had the privilege of serving as the Director of the National Security Agency (NSA) from 1992 to 1996, under President Clinton. In 1996, I retired from the U.S. Navy after 29 years of service - 26 of those years spent as a career Intelligence Officer. I then turned to the private sector as a consultant, where for ten years I worked to help the government achieve better results on a number of matters, including those concerning intelligence and national security. I have been in my current capacity as the nation's second Director of National Intelligence (DNI) since February 2007.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

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

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

### The Balance Achieved By FISA

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

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

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

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

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

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for

conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

### Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

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

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

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

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

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

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

### National Security Threats

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

Allow me to dispel that notion.

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

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at [dni.gov](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 Judiciary Committee of the House of Representatives, along with appropriately cleared professional staff.

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

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

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

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

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

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

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

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



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

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

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

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

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

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

Also on September 20, 2007, I was joined by National Security Agency Director (NSA), Lieutenant General Keith Alexander; Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division; Acting Assistant Attorney General from the Department of Justice's Office of Legal Policy, Brett Gerry; Federal Bureau of Investigation (FBI) Deputy Director John Pistole and the General Counsels of the ODNI, FBI, and NSA to speak to a closed session of the Select Committee on Intelligence of the Senate on the Protect America Act.

Additional Member and staff briefings shall follow.

#### Lasting FISA Modernization

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

#### Making the Changes Made by the Protect America Act Permanent

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

#### Liability Protection

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

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

#### Streamlining the FISA Process

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

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

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

Mr. Chairman, this concludes my remarks.