



# Department of Justice

---

STATEMENT OF

KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

OCTOBER 31, 2007

OLA-1A

**STATEMENT OF  
KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**

**OCTOBER 31, 2007**

Chairman Leahy, Ranking Member Specter, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as “FISA”). We appreciate the attention that Congress has given to this issue and the process that has led to the thoughtful bipartisan bill voted out of the Intelligence Committee on October 18, 2007, The FISA Amendments Act of 2007 (S. 2248).

Introduction

As you are aware, the Government’s foreign intelligence surveillance activities are a vital part of its efforts to keep the nation safe from international terrorists and other threats to the national security. These surveillance activities provide critical information regarding the plans and identities of terrorists who conspire to kill Americans at home and abroad, and they allow us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support—information that is key to tracking these organizations and disrupting their operations. In addition, our surveillance activities allow us to collect intelligence on the

intentions and capabilities of other foreign adversaries who pose a threat to the United States.

Prior to the passage of the Protect America Act of 2007 (PAA) in August, the difficulties we faced with FISA's outdated provisions—*i.e.*, the extension of FISA's requirements to surveillance targeting foreign intelligence targets overseas—substantially impeded the Intelligence Community's ability to collect effectively the foreign intelligence information necessary to protect the Nation. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May.

Recognizing the need to address this issue, Congress passed the Protect America Act, and the President signed the Act on August 5, 2007. The authorities you provided in the Protect America Act have allowed our intelligence agencies to collect vital foreign intelligence information, and the Act already has made the Nation safer by enabling the Intelligence Community to close gaps in our foreign intelligence collection. That Act, however, will expire in three months. To ensure that the Intelligence Community can obtain the information it needs to keep the Nation safe, the Administration strongly supports the reauthorization of the core authorities provided by the Protect America Act.

In addition, we urge Congress to enact the other important reforms to FISA contained in the proposal the Administration submitted to Congress in April; in particular, it is imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11<sup>th</sup> attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

We value the opportunity to work closely with Congress on these important issues. Since the passage of the Protect America Act, Congress has held numerous hearings on the implications of that Act, the scope of the authorities granted by that Act, and other issues related to FISA modernization, and various officials from the Executive Branch have testified repeatedly on the need to reauthorize the Act. Since September, I have testified on this issue before the Senate Intelligence Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee. Officials of the Executive Branch also have participated in numerous other meetings with Members and staff on this important topic.

In the Senate, this valuable process has culminated in the strong bipartisan bill referred to this Committee, S. 2248, and we applaud Congress for its initiative on this issue and its willingness to consult with us as it moves forward on FISA modernization. I am happy to be here today to continue the public discussion on this topic, and I look forward to working with this Committee as it considers S. 2248.

We still are reviewing S. 2248, which was voted out of committee on a bipartisan 13-2 vote two weeks ago, but we believe it is a balanced bill that includes many sound provisions that would allow our Intelligence Community to continue obtaining the information it needs to protect the nation. We therefore are optimistic that S. 2248 will lead to a bill the President can sign. We do, however, have concerns with certain provisions in S. 2248 and we look forward to working with this Committee and Congress to address those concerns and achieve lasting FISA reform.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be modernized, and I will explain how we have implemented the Protect America Act. I also will discuss our views on certain provisions of The FISA Amendments Act of 2007 (S. 2248)

and explain why that bill is superior to H.R. 3773. While we appreciate the work of the House of Representatives in holding hearings and considering the challenges posed by the outdated provisions of FISA, H.R. 3773 is problematic in several respects, and if that bill is presented to the President in its current form, his senior advisers and the DNI will recommend that he veto it.

### The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a “statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.” H.R. Rep. No. 95-1283, pt. 1, at 22 (1978). The law authorized the Attorney General to make an application to a newly established court—the Foreign Intelligence Surveillance Court (or “FISA Court”)—seeking a court order approving the use of “electronic surveillance” against foreign powers or their agents.

FISA established a regime of judicial review for foreign intelligence surveillance activities—but not for all such activities; only for certain of those that most substantially implicated the privacy interests of people in the United States. Congress designed a judicial review process that would apply primarily to surveillance activities within the United States—where privacy interests are the most pronounced—and not to overseas surveillance against foreign intelligence targets—where cognizable privacy interests are minimal or non-existent. The intent of Congress generally to exclude these intelligence activities from FISA’s reach is expressed clearly in the House Permanent Select Committee on Intelligence’s report, which explained: “[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances.” *Id.* at 27.

As a result of changes in telecommunications technology since 1978, however, the scope of activities covered by FISA expanded—without any conscious choice by Congress—to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA’s scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this requirement of obtaining a court order slowed, and in some cases may have blocked, the Government’s efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA’s reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

#### The Protect America Act of 2007

To address this and other problems and deficiencies in the FISA statute, the Administration submitted its FISA modernization proposal to Congress this April. Although Congress has yet to conclude its consideration of the Administration’s proposal, you took a significant step in the right direction by passing the Protect America Act in August. By updating the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably

believed to be outside the United States, the Protect America Act amended FISA to exclude from its scope those acquisitions directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation. The passage of the Protect America Act represented the right policy solution—allowing our intelligence agencies to surveil foreign intelligence targets located outside the United States without prior court approval—and one that is consistent with our Constitution.

(1) Our Use of this New Authority

Our experience since the passage of the Protect America Act has demonstrated the critical need to reauthorize the Act's core authorities and we urge Congress to make those provisions permanent. Prior to the passage of the Act, the Director of National Intelligence testified that the Intelligence Community was unable to obtain the foreign intelligence information, including information from terrorist communications, that it needed to collect in a timely manner in order to protect Americans from national security threats.

The authority provided by the Protect America Act has allowed us temporarily to close intelligence gaps that were caused by FISA's outdated provisions. I understand that since the passage of the Act, the Intelligence Community has collected critical intelligence important to preventing terrorist actions and enhancing our national security. The Intelligence Community needs to be able to continue to effectively obtain information of this nature if we are to stay a step ahead of terrorists who want to attack the United States, and Congress should make the core provisions of the Protect America Act permanent.

(2) Oversight of the PAA Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office and other oversight organizations, *e.g.*, Office of Inspector General and Office of General Counsel, of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews are conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, agencies using this authority are under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

(3) Congressional Reporting About Our Use of the PAA Authority

We also are reporting to Congress about our implementation and use of this new authority in a manner that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with



the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and properly cleared staff on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

We already have provided the Committee with documents related to our implementation of this new authority and have briefed appropriately cleared Committee staff members on PAA implementation issues. We also have completed several compliance reviews and are prepared to brief you on those reviews whenever it is convenient for you. Agencies employing this authority also continue to conduct on-site briefings, where Members and appropriately cleared staff have the opportunity to see how the Act has been implemented and to ask questions of those in the front lines of using this authority.

I am confident that this regime of oversight and congressional reporting will demonstrate

that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

S. 2248: The FISA Amendments Act of 2007

As you know, the Senate Select Committee on Intelligence voted a bill out of committee two weeks ago with strong bipartisan support, and we are continuing to review that bill—The FISA Amendments Act of 2007 (S. 2248). We believe the bill is generally a strong piece of legislation, and that it includes a number of important revisions to FISA.

(1) Core Collection Authority

First, like the PAA, S. 2248 would allow our intelligence professionals to collect foreign intelligence against targets located outside the United States without obtaining prior court approval. This represents the same fundamental policy judgment underlying the Protect America Act—that our intelligence agencies should be able to collect foreign intelligence on targets located outside the United States without prior court approval. It has been clear throughout this process that there is a general consensus that the Government should not be required to obtain a court order to acquire foreign intelligence on targets located abroad, and we strongly support reauthorization of the authority to collect intelligence on targets located outside the United States without prior court approval.

(2) Retroactive Immunity

Second, section 202 of S. 2248 would afford retroactive immunity from private lawsuits for those companies alleged to have assisted the Government in the aftermath of the September 11<sup>th</sup> attacks. Electronic communication service providers (“providers”) have faced numerous lawsuits as a result of their alleged activities in support of the Government’s efforts to prevent another terrorist attack. It is imperative that this provision be retained in this bill.

We believe that this is a just result. Any company that assisted the Government in defending our national security deserves our gratitude, not an avalanche of lawsuits. As the Senate Intelligence Committee noted in its report, the pending suits “seek hundreds of billions of dollars in damages from electronic communication service providers.” S. Rep. No. 110-209, at 8 (2007) (hereinafter “Sen. Rep.”). Under the proposal, a judge would dismiss a suit only if one of two circumstances is met: (1) the alleged assistance was not provided; or (2) the alleged assistance was in connection with an intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; was designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and was described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was authorized by the President and determined to be lawful. S. 2248, § 202.

After reviewing the relevant documents, and without identifying either the specific companies or the activities for which the companies provided assistance, the Intelligence Committee concluded that the providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. Sen. Rep. at 10. Because the committee “concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received,” *id.* at 11, the committee concluded that the providers “should be entitled to protection from civil suit.” *Id.* The committee’s considered judgment reflects a principle in the common law that private citizens who respond, in good faith, to a request for assistance by public officials should not be held liable for their actions.

In addition to being the just outcome, providing this litigation protection is important to the national security. Companies in the future may be less willing to assist the Government if they face litigation each time they are alleged to have provided assistance. As the Intelligence Committee noted in its report, “electronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies.” *Id.* Because of the need for such cooperation in the future and the extent of the lawsuits that have been filed, that committee concluded that retroactive immunity was a necessity.

Given the scope of the civil damages suits, and the current spotlight associated with providing any assistance to the intelligence community, the Committee was concerned that, without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. *The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.*

*Id.* (emphasis added). We are encouraged by that committee’s recognition that retroactive immunity is necessary to ensure timely cooperation from providers.

Further, allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods. The Intelligence Committee recognized in its report that this information should not be disclosed publicly.

[T]he identities of persons or entities who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence. . . . It would inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance.

Sen. Rep. at 10. Our adversaries can be expected to use such information to their benefit, and we should not allow them to benefit from this needless litigation. The prevention of such disclosures also is important to the security of the facilities and personnel of relevant electronic

communication service providers. The retroactive immunity provision in S. 2248 would ensure that cases against private entities falling within its terms will be dismissed and would help prevent the disclosure of highly classified information.

The Intelligence Committee's decision to provide retroactive immunity to electronic communication service providers also reflects a recognition that indemnification—whereby the Government would be responsible for any damages awarded against the providers—is not a workable response to the extensive litigation these companies face. First, even if they receive indemnification, the relevant companies would still face the burden of litigation. After all, they would still be parties to the lawsuits, and all of the potential litigation burdens would still fall on them as parties. Second, even if they would no longer face the possibility of an award of damages, the relevant companies could suffer damage to their business reputations and stock prices as a result of such litigation. Finally, as discussed above, allowing these cases to continue risks the further disclosure of highly classified information regarding intelligence sources and methods.

Similarly, substitution—whereby the Government would litigate in place of the electronic communication service providers—is not a workable solution. Although the providers would no longer be parties to the litigation, in order to prove their claims, the plaintiffs in these cases will certainly continue to seek discovery (through document requests, depositions, and similar means) from the providers. Thus, like indemnification, substitution would still place a burden of discovery on the companies, risk damaging their business reputations and stock prices, and risk the disclosure of highly classified information. Moreover, both indemnification and substitution could result in a tremendous waste of taxpayer resources on these lawsuits.

The Intelligence Committee’s decision to include retroactive immunity in the bill reflects a recognition that retroactive immunity is the best solution to the extensive litigation faced by the relevant companies. Indeed, the Committee rejected an amendment to strike Title II of the bill, which includes the immunity provision, on a 12-3 vote, and it is imperative that this provision be retained in the bill.

(3) Other Provisions Related to Litigation

Third, the bill contains several other beneficial provisions related to litigation and state investigations. Section 203 of S. 2248 provides a “procedure that can be used in the future to seek dismissal of a suit when a defendant either provided assistance pursuant to a lawful statutory requirement, or did not provide assistance.” Sen. Rep. at 12. As the Intelligence Committee noted, where a defendant has provided assistance to the Government pursuant to a lawful statutory requirement, but it would harm the national security for the request or assistance to be disclosed, such a procedure is a logical and expeditious way to achieve dismissal of such cases in the future. *Id.* In addition, section 204 of the bill would preempt state investigations or required disclosures of information—another important step in protecting highly classified information regarding classified sources and methods.

(4) Streamlining Provisions

Finally, sections 104 through 108 of S. 2248 would streamline the FISA application process in several positive ways. While FISA should require the Government, when applying for a FISA Court order, to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives. Among other things, the relevant sections of S. 2248 would eliminate unnecessary paperwork, while ensuring that the FISA Court has the information it

needs to process applications. As the Intelligence Committee stated in its report, these changes generally “are intended to increase the efficiency of the FISA process without depriving the Foreign Intelligence Surveillance Court of the information it needs to make findings required under FISA.” Sen. Rep. at 21.

Those sections also would make other improvements to FISA, such as increasing the time the Government has to file an application for a court order after authorizing emergency surveillance. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. S. 2248 would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately 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. While we are encouraged by the progress that has been made on reauthorization of the Protect America Act authorities, we still have concerns with certain provisions of S. 2248.

(5) United States Persons Located Outside the United States

First, we strongly oppose proposed subsection 703(c) of that bill, which would introduce a new role for the FISA Court with respect to collecting intelligence from United States persons located outside the United States.

It is unwise to extend this new role to the FISA Court. Traditionally, surveillance of United States persons overseas has been regulated by a time-tested Executive Branch process under Executive Order 12333. That executive order requires the Attorney General to make an individualized probable cause determination before the Government may conduct foreign intelligence surveillance on a United States person overseas. Prior to authorizing the use of such

techniques, the Attorney General must determine that there is probable cause to believe that the United States person being targeted is a “foreign power” or “agent of a foreign power.” These procedures, which have successfully balanced Americans’ privacy interests with the national security for over 25 years, were unchanged by the Protect America Act.

It would be a significant departure to extend the role of the FISA Court and require the Government to obtain the approval of the court to collect foreign intelligence regarding United States persons overseas. The Government is not required to obtain a warrant to collect evidence outside the United States when its purpose is to build a criminal case—where the expected end of the investigative process is often the criminal prosecution of that United States person. It makes little sense to create a court approval requirement in the context of foreign intelligence collection—when the objective is the defense of our national security and operational flexibility and speed are critical to achieve that objective. Congress did not create this role for the FISA Court when it enacted FISA in 1978, and it should not extend the court’s role in that regard in this legislation.

Subsection 703(c) of S. 2248, which would require the Attorney General to submit an application to the FISA Court to conduct an acquisition targeting a United States person overseas and to obtain a court order approving the acquisition prior to initiating it, also could have unintended consequences. First, unlike the current provisions of FISA governing electronic surveillance and physical searches, subsection 703(c) does not allow acquisitions regarding United States persons overseas to begin before obtaining court approval in emergency situations. Without an emergency provision, this subsection could impede operations and would result in the anomalous situation that it would be more difficult to surveil a United States person outside the country than inside the country. Second, extending this new role to the FISA Court and



requiring the court to approve acquisitions abroad could cause that court to feel compelled to analyze questions of foreign law as they relate to acquisitions under subsection 703(c), which could significantly complicate these types of collections and inject unpredictability into the process. We look forward to working with the Congress on this subsection as it considers S. 2248.

6. Sunset Provision

We also are opposed to the sunset provision in S. 2248 (section 101(c)), which would cause important provisions of the bill to sunset on December 31, 2013. In certain circumstances, a sunset provision may make sense. Where Congress enacts significant changes to existing legal authorities without the opportunity for sufficient deliberation or fact-finding, a sunset provision can afford Congress the chance to evaluate the effect of certain legislation. For example, the PATRIOT Act, which was enacted very quickly after the September 11<sup>th</sup> attacks, included sunset provisions and we recognize why Congress chose to include sunset provisions in that legislation. We also understand why Congress chose to include a sunset provision in the Protect America Act, which was similarly passed in response to a compelling and immediate need.

In contrast, a sunset provision should not be included in S. 2248, which would reauthorize the core authorities Congress included in the Protect America Act. There has been extensive public discussion and consideration of FISA modernization and the Protect America Act, both before and after passage of that Act in August. There is now a lengthy factual record on the need for FISA modernization, the implementation of the Protect America Act, the implications of the core authorities under the Act, and the appropriate level of Congressional oversight of this authority. Executive Branch officials have testified at numerous hearings over the last two years and conducted countless briefings for Members and staff on the need for FISA

modernization and the implementation of the Protect America Act. In addition, the Executive Branch has provided Congress with extensive information regarding the implementation of the Act—information that went well beyond that required by the statute. This has provided a track record of our implementation of the Protect America Act authority and has afforded Congress the opportunity to study this issue extensively. As the Intelligence Committee explained, S. 2248 reflects the culmination of a long process of hearings, classified briefings, and the review of relevant documents. S. Rep. at 2-3. Given the extensive factual record and public debate on these issues, the sunset provision in S. 2248 is not necessary.

We oppose the sunset provision because it introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners. It is inefficient and unworkable for agencies to develop new processes and procedures and train their employees, only to have the law change within a period of several years. The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not in a persistent state of doubt.

#### 7. Reporting and Oversight Provisions

We are continuing to analyze the increased reporting and oversight requirements in S. 2248 to determine whether they strike a workable balance between Congress's need for information concerning intelligence activities and the dedication of resources necessary to meet those reporting requirements. We value Congressional oversight of the Protect America Act authorities and we understand that oversight is necessary to demonstrate publicly that we are employing the authorities responsibly, as was made clear by our decision to exceed substantially the Congressional reporting requirements under the Act.

We are, however, troubled by certain provisions of S. 2248, which may pose significant burdens on our intelligence agencies. For example, subsection 703(l) requires, among other things, an annual review to determine “the number of persons located in the United States whose communications were reviewed.” S. 2248, § 703(l). Given the fragmentary nature of foreign intelligence collection and the limited amount of information available concerning any specific intercepted communication, I am informed that it would likely be impossible for intelligence agencies to comply with this requirement.

#### H.R. 3773

In contrast to S. 2248, the legislation introduced in the House of Representatives—H.R. 3773—falls short of providing the Intelligence Community with the tools it needs to collect foreign intelligence effectively from individuals located outside the United States. While we appreciate the efforts of the House to introduce a bill on this topic, we believe H.R. 3773 would be a step backward for national security. As the Administration has stated, if H.R. 3773 is presented in its current form to the President, the Director of National Intelligence and the President’s other senior advisers will recommend that he veto the bill.

H.R. 3773 is deficient in several respects. First, it would limit the type of foreign intelligence information that could be acquired under its authority. Since 1978, FISA has provided for the collection of foreign intelligence information, and there is no reason to place complex restrictions on the types of intelligence that can be collected from persons outside the United States under this authority. This limitation would serve only to require intelligence analysts to spend valuable time and resources in distinguishing between types of foreign intelligence information being collected.

Second, H.R. 3773 does not provide retroactive liability protection to electronic communication service providers or federal preemption of state investigations. As discussed above and recognized by the Senate Intelligence Committee in its report, those companies alleged to have assisted the Government in the aftermath of September 11<sup>th</sup> should not face litigation over those matters. Such litigation risks the disclosure of highly classified information and could lead to reduced intelligence collection capabilities in the future by discouraging companies from cooperating with the Government.

Third, in contrast to the Protect America Act and S. 2248, H.R. 3773 would require prior court approval for acquisitions of foreign intelligence information on targets located overseas absent an emergency. This is a significant increase in the role of the FISA Court with respect to the authorities provided by the Act and it could impede the collection of necessary foreign intelligence information. In addition, these provisions would not provide any meaningful increase in the protection of the privacy interests of Americans in the United States. H.R. 3773 also fails explicitly to provide for continued intelligence collection while the Government appeals an order of the FISA Court.

Finally, H.R. 3773 would sunset in a little over two years. As discussed above, intelligence agencies need certainty and permanence in the rules they employ for intelligence collection and we oppose any sunset provision. We are strongly opposed to the extremely short sunset provision in H.R. 3773.

While we look forward to working with Congress towards the passage of a permanent FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting the constitutional rights of Americans, we cannot support H.R. 3773 in its current form.

## Conclusion

The Protect America Act has been critical to our efforts to gather the foreign intelligence information necessary to protect the Nation, and it is crucial that its core aspects be made permanent. In addition to making the core provisions of the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We are encouraged by the progress that has been made on this issue, particularly with respect to many of the provisions in S. 2248, and we look forward to working with Congress and this Committee as it considers S. 2248.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.



# Department of Justice

---

STATEMENT OF

KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE  
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 20, 2007

ES-7A

**STATEMENT OF  
KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

**SEPTEMBER 20, 2007**

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. We urge the Congress to make the Protect America Act permanent, and also to enact the other important reforms to FISA contained in the Administration's proposal. It is especially imperative that

Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several concerns and misunderstandings that have arisen regarding the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

#### The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a “statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.”<sup>1</sup> The law authorized the Attorney General to make an application to a newly established court—the Foreign Intelligence Surveillance Court (or “FISA Court”)—seeking a court order approving the use of “electronic surveillance” against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA’s regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA’s reach is expressed clearly in the House Permanent Select Committee on Intelligence’s report, which explained: “[t]he committee has explored the

---

<sup>1</sup> H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).



feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances.”<sup>2</sup>

The mechanism by which Congress gave effect to this intent was its careful definition of “electronic surveillance,” the term that identifies which Government activities fall within FISA’s scope. This statutory definition is complicated and difficult to parse, in part because it defines “electronic surveillance” by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA’s use of technology-dependent provisions that has caused FISA to apply to activities today that its drafters never intended.)

The original definition of electronic surveillance is the following:

(f) "Electronic surveillance" means-

- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
- (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
- (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from

---

<sup>2</sup> *Id.* at 27.

a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.<sup>3</sup>

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition of “the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA’s scope, period.

Further analysis of that definitional language also demonstrates the opposite—that surveillance-targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as “radio” (vs. “wire”) communications. Under the statutory definition, surveillance of these international/“radio” communications would become “electronic surveillance” only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of “electronic surveillance”);<sup>4</sup> or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that “both the sender and all intended recipients are

---

<sup>3</sup> 50 U.S.C. 1801 (f).

<sup>4</sup> 50 U.S.C. 1801 (f)(1).

in the United States”).<sup>5</sup> Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in “electronic surveillance” and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

As satellite (“radio”) gave way to transoceanic fiber optic cables (“wire”) for the transmission of most international communications and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA’s scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government’s efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA’s reach also necessarily

---

<sup>5</sup> At the time of FISA’s enactment, the remaining two definitions of “electronic surveillance” did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to “wire communications,” which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA’s drafters explained was “not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States.” H.R. Rep. No. 95-1283 at 52.

diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The legislative package we submitted in April proposed to fix this problem by amending the definition of “electronic surveillance” to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA’s privacy protections on persons located in the United States.

#### The Protect America Act of 2007

Although Congress has yet to conclude its consideration of the Administration’s proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration’s proposal. It is particularly critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

By updating the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows

the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the information from or with the assistance of a communications service provider, custodian, or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B concern persons reasonably believed to be outside the United States and therefore do not constitute electronic surveillance. The FISA Court then must review the Government's

determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us to close existing gaps in our foreign intelligence collection that were caused by FISA's outdated provisions.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide reporting to Congress about our implementation and use of this new authority that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

We already have completed two compliance reviews and are prepared to brief you on those reviews whenever it is convenient for you.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Concerns and Misunderstandings about the New Authority

I also want briefly to address some of the concerns and misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of this Committee during the September 6, 2007, hearing, we sent a letter to the Committee that clearly outlines the position of the Executive Branch on several such issues. We hope that the letter dispels any concerns or misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement.

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. As I explained at a hearing of the House Judiciary Committee on September 18, 2007, the Act leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words,



the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." I reiterated this conclusion at the House Judiciary Committee hearing on September 18, 2007—the statute simply does not

authorize these activities.

Section 105B was intended to provide a mechanism for the government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information “from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications.” Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that “where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.” 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and

personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute “electronic surveillance” under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, this provision does not authorize the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they “concern” persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, some have expressed concerns that the Protect America Act authorizes so-called “reverse targeting” without a court order. It would be “reverse targeting” if the Government were to surveil a person overseas where the Government’s actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute “electronic surveillance” under FISA—because it would involve the acquisition of communications to or from a U.S. person in the United States “by intentionally targeting that United States person,” 50 U.S.C. § 1801(f)(1)—and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect

America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. I reiterated this position at the House Judiciary Committee hearing on September 18, 2007. Because it would remain a violation of FISA, the Government cannot—and will not—use this authority to engage in “reverse targeting.”

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in “reverse targeting.” If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target’s calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target’s communications.

Additionally, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA’s scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community’s long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order

12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in

1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas—a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

#### The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. Second, Congress should provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. Third, it is important that Congress consider and

ultimately pass other provisions in our proposal. These provisions—which draw from a number of thoughtful bills introduced in Congress during its last session—would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of “agent of a foreign power”—a category of individuals the Government may target with a FISA court order—to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.
- The bill would provide a mechanism by which third parties—primarily telecommunications providers—could challenge a surveillance directive in the FISA Court.
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

#### Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. Additionally, it is critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. This important provision is contained in section 408 of our proposal. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed

change in the bill—both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent.

#### Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States. As detailed above, 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 actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-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 encompass: “(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.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.”

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can

collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community's ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

#### Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA 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. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which

these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of “foreign powers” to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of “minimization procedures” referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) 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. This is a critical change that works hand in glove with the new definition of “electronic surveillance” in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of “electronic surveillance,” certain activities that previously were “electronic surveillance” under FISA would fall out of the statute’s scope. This new provision would provide a mechanism for

the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of “electronic surveillance.” The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

### Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from “at least seven” of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court’s jurisdiction. The new provision would eliminate the restriction on the FISA Court’s jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

#### Section 404

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a “detailed description of the nature of the information sought,” and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a “statement of facts concerning all previous applications” involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new

provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this Committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

#### Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States 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-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately 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. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is “significant foreign intelligence information” that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of “contents” in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

#### Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must 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; we believe that the same rule should apply

regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired 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 would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

#### Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would 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 (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.” Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

#### Section 408

Section 408 would provide litigation protections to telecommunications companies who



are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11<sup>th</sup> terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

#### Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

#### Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843)

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.

#### Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court 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 FISA Court, 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 FISA Court 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.

#### Other Provisions

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

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 allow for a smooth transition after the proposed changes take effect.

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.

### Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.



# Department of Justice

---

STATEMENT OF

KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY  
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 18, 2007

OLA-10

**STATEMENT OF  
KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**

**SEPTEMBER 18, 2007**

Chairman Conyers, Ranking Member Smith, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. We urge the Congress to make the Protect America Act permanent, and also to enact the other important reforms to FISA contained in the Administration's proposal. It is especially imperative that

Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several concerns and misunderstandings that have arisen regarding the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

#### The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."<sup>1</sup> The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the

---

<sup>1</sup> H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances.”<sup>2</sup>

The mechanism by which Congress gave effect to this intent was its careful definition of “electronic surveillance,” the term that identifies which Government activities fall within FISA’s scope. This statutory definition is complicated and difficult to parse, in part because it defines “electronic surveillance” by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA’s use of technology-dependent provisions that has caused FISA to apply to activities today that its drafters never intended.)

The original definition of electronic surveillance is the following:

(f) “Electronic surveillance” means-

- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
- (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
- (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from

---

<sup>2</sup> *Id.* at 27.

a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.<sup>3</sup>

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition of “the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA’s scope, period.

Further analysis of that definitional language also demonstrates the opposite—that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as “radio” (vs. “wire”) communications. Under the statutory definition, surveillance of these international/“radio” communications would become “electronic surveillance” only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of “electronic surveillance”);<sup>4</sup> or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that “both the sender and all intended recipients are

---

<sup>3</sup> 50 U.S.C. 1801 (f).

<sup>4</sup> 50 U.S.C. 1801 (f)(1).



in the United States”).<sup>5</sup> Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in “electronic surveillance” and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

As satellite (“radio”) gave way to transoceanic fiber optic cables (“wire”) for the transmission of most international communications and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA’s scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government’s efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA’s reach also necessarily

---

<sup>5</sup> At the time of FISA’s enactment, the remaining two definitions of “electronic surveillance” did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to “wire communications,” which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA’s drafters explained was “not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States.” H.R. Rep. No. 95-1283 at 52.

diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The legislative package we submitted in April proposed to fix this problem by amending the definition of “electronic surveillance” to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA’s privacy protections on persons located in the United States.

#### The Protect America Act of 2007

Although Congress has yet to conclude its consideration of the Administration’s proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration’s proposal. It is particularly critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

By updating the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows

the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the information from or with the assistance of a communications service provider, custodian, or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B concern persons reasonably believed to be outside the United States and therefore do not constitute electronic surveillance. The FISA Court then must review the Government's

determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us effectively to close an intelligence gap identified by the DNI that was caused by FISA's outdated provisions.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide reporting to Congress about our implementation and use of this new authority that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

As I stated above, we already have completed the first compliance review and are prepared to brief you on that review whenever it is convenient for you.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Concerns and Misunderstandings about the New Authority

I also want briefly to address some of the concerns and misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of the House Permanent Select Committee on Intelligence after a September 6, 2007, hearing, we sent a letter to that Committee that clearly outlines the position of the Executive Branch on several such issues. We also sent a copy of that letter to this Committee and we hope that the letter dispels any concerns or misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement.

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words,

the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information “from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications.” Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that “where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.” 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for



such purposes.

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, this provision does not authorize the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, some have expressed concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA—because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1)—and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance

directed at targets overseas. Because it would remain a violation of FISA, the Government cannot—and will not—use this authority to engage in “reverse targeting.”

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in “reverse targeting.” If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target’s calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target’s communications.

Additionally, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA’s scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community’s long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order 12333. There is no principled rationale for requiring a court order to surveil these suspects’ communications when we intercept them in the United States when no court order is required for

surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of

judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

#### The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. Second, Congress should provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. Third, it is important that Congress consider and ultimately pass other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of

salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of “agent of a foreign power” - - a category of individuals the Government may target with a FISA court order -- to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.
- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court.
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

#### Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. Additionally, it is critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. This important provision is contained in section 408 of our proposal. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill -- both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent.

## Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States. As detailed above, 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 actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-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 encompass: "(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.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.”

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community’s ability to collect valuable

foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term “minimization procedures.” This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term “contents” consistent with the definition of “contents” as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of “contents” in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

#### Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA 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. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA.



As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of “foreign powers” to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of “minimization procedures” referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) 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. This is a critical change that works hand in glove with the new definition of “electronic surveillance” in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of “electronic surveillance,” certain activities that previously were “electronic surveillance” under FISA would fall out of the statute’s scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of “electronic surveillance.” The new

section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

#### Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from “at least seven” of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court’s jurisdiction. The new provision would eliminate the restriction on the FISA Court’s jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

#### Section 404

The current procedure for applying to the FISA Court for a surveillance order under

section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a “detailed description of the nature of the information sought,” and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a “statement of facts concerning all previous applications” involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this

committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

#### Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States 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-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately 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. This provision also would modify the existing

provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is “significant foreign intelligence information” that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of “contents” in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

#### Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must 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; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired 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 would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

#### Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would 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 (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.” Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

#### Section 408

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11<sup>th</sup> terrorist attacks. Telecommunications companies

have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

#### Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

#### Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) 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.

#### Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court 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 FISA Court, 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 FISA Court 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.

#### Other Provisions

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

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 allow for a smooth transition after the proposed changes take effect.

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.

#### Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.



# Department of Justice

---

STATEMENT OF

KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY  
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 18, 2007

**OLA-10B**

**STATEMENT OF  
KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**

**SEPTEMBER 18, 2007**

Chairman Conyers, Ranking Member Smith, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as “FISA”).

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration’s proposal. While I commend Congress for passing the Protect America Act of 2007 (the “Protect America Act”) in August, the Act is a partial solution that will expire in less than six months. Congress should make the Protect America Act permanent, and also make other important reforms to FISA contained in the Administration’s proposal—such as providing liability protection to companies

that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several misunderstandings about the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

#### The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."<sup>1</sup> The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select

---

<sup>1</sup> H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."<sup>2</sup>

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which Government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that we submit its drafters never intended.)

The original definition of electronic surveillance is the following:

(f) "Electronic surveillance" means-

- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
- (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

---

<sup>2</sup> *Id.* at 27.

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.<sup>3</sup>

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition of “the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA’s scope, period.

Further analysis of that definitional language also demonstrates the opposite—that surveillance targeting someone overseas was generally not intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as “radio” (vs. “wire”) communications. Under the statutory definition, surveillance of these “radio” - international communications would become “electronic surveillance” only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of “electronic surveillance”);<sup>4</sup> or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the

---

<sup>3</sup> 50 U.S.C. 1801 (f).

<sup>4</sup> 50 U.S.C. 1801 (f)(1).

third definition of electronic surveillance, i.e. that “both the sender and all intended recipients are in the United States”).<sup>5</sup> Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in “electronic surveillance” and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

As satellite gave way to wire and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA’s scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States. In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government’s efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA’s reach also necessarily

---

<sup>5</sup> At the time of FISA’s enactment, the remaining two definitions of “electronic surveillance” did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to “wire communications,” which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA’s drafters explained was “not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States.” H.R. Rep. No. 95-1283 at 52.

diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The legislative package we submitted in April proposed to fix this problem by amending the definition of “electronic surveillance” to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA’s privacy protections on persons located in the United States.

#### The Protect America Act of 2007

Although Congress has yet to conclude its consideration of the Administration’s proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration’s proposal—such as providing liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

By updating the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows



the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute “electronic surveillance,” and that the acquisition involves obtaining the information from or with the assistance of a communications service provider or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B do not constitute electronic surveillance. The FISA Court then must review the Government’s determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us effectively to close an intelligence gap identified by the DNI that was caused by FISA's outdated provisions. I can discuss this in more detail in a classified setting.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

I can provide specific details of our oversight efforts to date in a classified setting.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide reporting to Congress about our implementation and use of this new authority that exceeds the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods; and,
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B.
- Because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

As I stated above, we already have completed the first compliance review and are prepared to brief you on that review whenever it is convenient for you. The Government also

has conducted an on-site briefing for Committee staff members regarding implementation of the Act.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Misunderstandings about the New Authority

I also want briefly to address some of the misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of the House Permanent Select Committee on Intelligence after a September 6, 2007, hearing, we sent a letter to that Committee that clearly outlines the position of the Executive Branch on several such issues. We also sent a copy of that letter to this Committee and we hope that the letter dispels these misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement.

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct

electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the government to obtain third-

party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information “from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications.” Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that “where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.” 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute “electronic surveillance” under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, we do not think that this provision authorizes the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they “concern” persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, some have expressed concerns that the Protect America Act authorizes so-called “reverse targeting” without a court order. It would be “reverse targeting” if the Government were to surveil a person overseas where the Government’s actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute “electronic surveillance” under FISA—because it would involve the acquisition of communications to or from a U.S. person in the United States “by intentionally targeting that United States person,” 50 U.S.C. § 1801(f)(1)—and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. Because it would remain a violation of FISA, the Government

cannot—and will not—use this authority to engage in “reverse targeting.”

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in “reverse targeting.” If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target’s calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target’s communications.

Additionally, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA’s scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community’s long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order 12333. There is no principled rationale for requiring a court order to surveil these suspects’ communications when we intercept them in the United States when no court order is required for surveilling those very same communications (including communications between those suspects



and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons

overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

#### The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. We also believe that it is important that Congress consider and ultimately pass other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of “agent of a foreign power” - a category of individuals the Government may target with a FISA court order -- to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that

posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.

- The bill would afford litigation protections to telecommunications companies that have allegedly provided the Government with critical assistance in its efforts to surveil terrorists and protect the nation since the September 11<sup>th</sup> terrorist attacks.
- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court.
- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

#### Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill -- both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent.

#### Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States. As detailed above, 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 actually intended to *exclude* from FISA’s scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress’ original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-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 encompass: “(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.” Under this definition, FISA’s scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA’s scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between “wire” and “radio” communications that appears throughout the Act. Accordingly, the Administration’s proposal would strike FISA’s current definition of “wire communication,” because reference to that term is unnecessary under the new, technology neutral definition of “electronic surveillance.”

The proposal also would amend other definitions to address gaps in FISA’s coverage. Subsection 401(a) would amend FISA’s definition of “agent of a foreign power” to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community’s ability to collect valuable foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term “minimization procedures.” This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term “contents” consistent with the definition of “contents” as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of “contents” in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

#### Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA 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. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA. As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of “foreign powers” to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States

persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of “minimization procedures” referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) 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. This is a critical change that works hand in glove with the new definition of “electronic surveillance” in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of “electronic surveillance,” certain activities that previously were “electronic surveillance” under FISA would fall out of the statute’s scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of “electronic surveillance.” The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

#### Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from “at

least seven” of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court’s jurisdiction. The new provision would eliminate the restriction on the FISA Court’s jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

#### Section 404

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in



several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a “detailed description of the nature of the information sought,” and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a “statement of facts concerning all previous applications” involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration’s proposal would allow intelligence agencies to more expeditiously obtain certifications.

#### Section 405

Section 405 would amend the procedures for the issuance of an order under section 105

of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States 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-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately 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. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is “significant foreign intelligence information” that, while important to the security of the country, may not rise to the

level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of “contents” in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

#### Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must 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; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired 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 would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of

classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

#### Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would 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 (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of “foreign intelligence information.” Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

#### Section 408

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11<sup>th</sup> terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the Government’s efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

#### Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

#### Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) 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.

#### Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court 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 FISA Court, 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 FISA Court 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.

#### Other Provisions

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

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 allow for a smooth transition after the proposed changes take effect.

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.

## Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. This would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.

**Oral Statement of Kenneth L. Wainstein**

**on**

**The Foreign Intelligence Surveillance Act**

**before the**

**House Permanent Select Committee on Intelligence**

**September 6, 2007**

**OLA-137A**



**ORAL STATEMENT OF  
KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE**

**CONCERNING**

**THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

**BEFORE THE**

**PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

**SEPTEMBER 6, 2007**

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for this opportunity to testify concerning FISA modernization. I am proud to be here today to represent the Department of Justice and to discuss this important issue with you.

I'd like to take a few moments to explain why I think we need to permanently modernize the FISA statute. To do that, I will briefly discuss first what Congress intended to accomplish when it drafted FISA in 1978, and second how sweeping changes in telecommunications technology since then resulted in the requirements of FISA being extended to surveillance activities that Congress sought to exclude from the scope of FISA when it was enacted. I will then explain how this process impaired our intelligence capabilities and points up the need to modernize FISA on a permanent basis. Finally, I will briefly describe the efforts we are making to ensure that the temporary fix you adopted last month in the Protect America Act is implemented in a responsible and transparent manner.

### The FISA Congress Intended: The Scope of FISA in 1978

In enacting FISA, the Congress of 1978 established a regime of judicial review for foreign intelligence surveillance activities -- but not for all such activities; only for those that most substantially implicated the privacy interests of people in the United States. Striking a careful balance between the protection of privacy and the need for the effective collection of foreign intelligence, Congress designed a judicial review process that would apply primarily to surveillance activities within the United States -- where privacy interests are the most pronounced -- and not to overseas surveillance against foreign targets -- where cognizable privacy interests are minimal or non-existent.

Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," the term that identifies those Government activities that fall within the scope of the statute and, by implication, those that fall outside it. Congress established this dichotomy by defining "electronic surveillance" by reference to the *manner* of the communication under surveillance -- by distinguishing between "wire" communications -- which included most of the local and domestic traffic in 1978 -- and "radio" communications -- which included most of the transoceanic traffic in that era. Based on the communications reality of that time, that dichotomy more or less accomplished the Congressional purpose of distinguishing between domestic communications that generally fell within FISA and foreign international communications that generally did not.

### The Unintended Consequences of Technological Change

The revolution in communications technology since 1978 radically altered that reality and upset the careful balance in the statute. As a result, certain surveillance activities directed at persons overseas -- which were not intended to fall within FISA -- became subject to FISA, which required us to seek court authorization and effectively conferred quasi-constitutional

protections on terrorist suspects and other national security targets overseas. This process impaired our surveillance efforts and diverted resources that would have been better spent protecting the privacy interests of persons within the United States.

The Protect America Act of 2007

In April of this year, the Administration submitted to Congress a comprehensive proposal that would remedy this problem and provide a number of other important refinements to the FISA statute. While Congress has yet to act on the complete package we submitted, your passage of the temporary legislation in August was a significant step in the right direction. That legislation updated the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States, thereby restoring FISA to its original focus on domestic surveillance and allowing us the critical latitude to surveil overseas terrorists and other national security threats without going through a lengthy court approval process.

[The authority provided by the Act is an essential one and allowed us effectively to close an intelligence gap identified by the DNI that was caused by FISA’s outdated provisions.]

The legislation only lasts for six months, and the new authority is scheduled to expire on February 5, 2008, absent reauthorization. I see this interim period as an opportunity to do two things. First and foremost, it gives us the opportunity to demonstrate that we can use this authority responsibly, conscientiously and effectively. That is an opportunity that we have already started to seize. As we explained in a letter we sent the Committee this Tuesday, we have already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as on-site compliance reviews by a team from the Office of the Director of National Intelligence (ODNI) and the National Security Division of the Department of Justice. This DNI/NSD team has already completed its first audit, and it will complete further

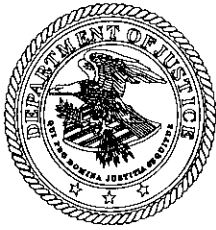
audits every 30 days during this interim period to ensure full compliance with the implementation procedures.

In that same letter, we also committed to providing Congress with comprehensive reports about how we are implementing this authority. We will make ourselves available to brief you and your staffs on the results of our regular compliance reviews; we will provide you copies of the written reports of those audits; and we will give you update briefings every month on compliance matters and on implementation of this authority in general. In fact, we are prepared to brief you on the first compliance review whenever it is convenient for you.

We are confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority, and that it will demonstrate that you made the absolutely right decision when you passed the Protect America Act last month.

This interim period also gives us one other opportunity -- the opportunity to engage in a serious debate and dialogue on this important issue. I feel strongly that American liberty and security were advanced by the Act, and that they will be further advanced by adoption of our comprehensive FISA Modernization proposal. However, I recognize that this is a matter of significant and legitimate concern to many throughout our country. For that reason, this Committee is wise to hold this hearing and to explore the various legislative options and their implications for national security and civil liberties. I am confident that, when those options and implications are subject to objective scrutiny and to honest debate, Congress and the American people will see both the wisdom and the imperative of modernizing the FISA statute on a permanent basis.

Thank you again for the opportunity to appear before you. I look forward to answering your questions.



# Department of Justice

---

STATEMENT OF

KENNETH L. WAINSTEIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE  
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 6, 2007



U.S. Department of Justice

National Security Division

Assistant Attorney General

Washington, D.C. 20530

SEP 14 2007

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

Dear Chairman Reyes:

I write this letter in response to questions posed by you and other Members of the House Permanent Select Committee on Intelligence at its hearing on September 6, 2007, concerning the scope of the Protect America Act of 2007. You requested that certain answers given at that hearing be provided in writing and -- to the extent possible consistent with the national security -- in an unclassified format.

I appreciate your invitation to provide our thoughts on these matters as you evaluate the Protect America Act and consider our request to make the legislation permanent. I believe that this dialogue is a healthy process, and that it will help provide assurance to the American public and the Congress that the Act is a measured and sound approach to an important intelligence challenge.

The passage of the Protect America Act was a significant step forward for our national security. As this Committee is aware, sweeping changes in telecommunications technologies since the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978 expanded the scope of the statute substantially. As a result of these technological changes -- and not of any deliberate choice by the Congress -- the Executive Branch frequently was required to seek court approval, based upon a showing of probable cause, to conduct surveillance targeting terrorists and other foreign intelligence targets located overseas. This created a significant gap in our intelligence capabilities with no corresponding benefit to the civil liberties of persons in the United States.

By changing FISA's definition of electronic surveillance to clarify that the statute does not apply to surveillance directed at overseas targets, the Congress has enabled the Intelligence Community to close critical intelligence gaps, and the nation is already safer because of it. We urge the Congress to make the Protect America Act permanent, and also to enact the other important FISA reforms contained in the comprehensive FISA Modernization proposal we submitted to Congress earlier this year. It is especially imperative that Congress provide liability protection to companies that are alleged to have

**DAG-117A**

assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

At the hearing last week, you and other Members of the Committee asked several specific questions concerning whether the Protect America Act hypothetically could authorize the Government to engage in certain intelligence activities that extend beyond those you contemplated when Congress passed the legislation. We appreciate the opportunity to provide you with answers, as these and other such questions have also been asked by other members of Congress and by members of the public.

While we understand the civil liberties concerns underlying these various questions, there are several reasons why this legislation does not give rise to these concerns. First, most of the hypotheticals we have heard are inconsistent with the plain language of the Protect America Act and the rest of the FISA statute. Second, we commit that we will not use the statute to undertake intelligence activities that extend beyond the clear purpose of the statute. And third, we will apply the statute in the full view of congressional oversight, as we intend to provide Congress with consistent and comprehensive insight into our implementation and use of this authority. As we have publicly committed, we will inform the full membership of the Intelligence and Judiciary Committees concerning the implementation of this new authority and the results of the reviews that this Division and the Office of the Director of National Intelligence are conducting to assess and ensure compliance by the implementing agencies; we will provide you copies of the written reports of those compliance reviews; and we will make ourselves available to brief you and your staffs about compliance and implementation on a monthly basis throughout this renewal period. In fact, representatives of the Executive Branch already have provided several detailed briefings to Committee Members and staff on the implementation of the Protect America Act since its passage. In addition, we have provided the committees with copies of documents related to our implementation of this authority, including the relevant certifications and procedures required by the statute (with redactions as necessary to protect critical intelligence sources and methods). With such comprehensive reporting to Congress, you and your colleagues will be able to see and assure yourselves that we are implementing this new authority appropriately, responsibly, and only in furtherance of the purposes underlying the statute.

\*\*\*\*\*

I would like to address several of the hypothetical situations you and your colleagues raised at the hearing last week, and explain why we believe they will not arise under our implementation of the Protect America Act.

*First*, questions arose at the hearing concerning the Protect America Act's application to domestic communications, and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located

*outside of the United States,*" Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2) -- a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

*Second*, several Members of the Committee asked whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the Government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).



Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications -- further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

*Third*, a question was asked about whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, we do not think that this provision authorizes the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

*Fourth*, and finally, it was suggested that this letter be used as an opportunity for the Executive Branch to allay concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA -- because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1) -- and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. Because it would remain a violation of FISA, the Government cannot -- and will not -- use this authority to engage in "reverse targeting."

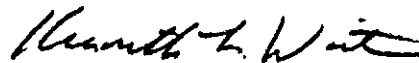
It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in "reverse targeting." If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target's calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target's communications.

\*\*\*\*\*

Thank you again for the opportunity to appear at your hearing last week, and to provide these responses to your thoughtful questions. I hope you find this input helpful. Because we believe that these responses will likely be of interest to the Senate Select Committee on Intelligence and the Judiciary Committees, I have sent copies of this letter to the Chairman and Ranking Member of each of those committees.

Please do not hesitate to call on me or my colleagues if we can be of further assistance as you consider FISA modernization and the renewal of the Protect America Act.

Sincerely,



Kenneth L. Wainstein  
Assistant Attorney General

cc: Sen. Rockefeller  
Sen. Bond  
Sen. Leahy  
Sen. Specter  
Rep. Hoekstra  
Rep. Conyers  
Rep. Smith