Testimony of

# Kenneth L. Wainstein

October 31, 2007

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Prior to the passage of the Protect America Act of 2007 (PAA) in August, the difficulties we faced with FISA's outdated provisions--i.e., the extension of FISA's requirements to surveillance targeting foreign intelligence targets overseas--substantially impeded the Intelligence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 11th 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 11th 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 11th 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 11th 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.