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

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."[1] 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

[1] 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."[2]

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

[2] *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.[3]

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 <u>not</u> 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");[4] 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

[3] 50 U.S.C. 1801 (f).
[4] 50 U.S.C. 1801 (f)(1).

in the United States").[5] 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

[5] 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 11th 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.