Department of Justice

STATEMENT OF

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

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

CONCERNING

THE NEED TO BRING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT INTO THE MODERN ERA

PRESENTED

May 1, 2007

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

CONCERNING

THE NEED TO BRING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT INTO THE MODERN ERA

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

MAY 1, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, I want to thank you for this opportunity to testify in a public setting concerning the Administration's proposal to modernize the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

In order to explain why we must modernize FISA today, it is important to understand what Congress intended to accomplish when it drafted FISA almost thirty years ago. I will therefore begin my testimony today with a brief discussion of the context in which FISA was enacted. Then I will explain how sweeping changes since 1978—both in the nature of the threat that we face and in telecommunications technologies—have upset the delicate balance that Congress sought to achieve when it enacted FISA. As a result of these changes, FISA now regulates many intelligence activities of the sort that Congress sought to exclude from the scope of FISA—an unintended consequence that has impaired our intelligence capabilities. I will conclude by providing the Committee a detailed, but unclassified, explanation of the specific reforms of the statute that we believe are needed to restore FISA to its original focus. By

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.

The FISA Congress Intended: The Scope of FISA in 1978

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 legislation came on the heels of the Church Committee Report, which disclosed abuses of domestic national security surveillances, and reflected a judgment that the civil liberties of Americans would be well-served by the development of a process for court approval of foreign intelligence surveillance activities directed at individuals in the United States. To accomplish this objective, Congress 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.

However, in making these changes, Congress recognized the importance of striking an appropriate balance between the need to protect the civil liberties of Americans, and the imperative that the Government be able to collect effectively foreign intelligence information that is vital to the national security.[2] It also recognized that the terrain in which it was legislating touched upon a core Executive Branch function—the Executive's constitutional responsibility to protect the United States from foreign threats.[3] Congress attempted to accommodate these potentially competing concerns by applying FISA's process of judicial approval to certain

[1] H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).
[2] *Id*. at 21, 22, 25.
[3] *See, e.g.*, *id*. at 15 (referring to "the President's constitutional powers to gather intelligence deemed necessary to the security of the nation").

intelligence 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 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."[4]

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that we submit its drafters never intended.) The fact that many of the intelligence activities at issue are highly classified further complicates any effort to explain these provisions in an unclassified setting.

By reading the plain text of these provisions in light of the telecommunications communications technologies available at the time of FISA's passage, however, we can learn a great deal both about what Congress intended to cover and about what intelligence activities it intended to exclude from FISA. Consider at the outset the first 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

[4] *Id*. at 27.

States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[5] In other words, if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence purposes, it is within FISA's scope, period.

A close reading of FISA's definition of "electronic surveillance" in context makes a related point clear: if the Government directed surveillance at the communications of a person overseas, those acquisitions were generally excluded from FISA's scope. The key here is the third definition of electronic surveillance, which encompasses the acquisition of "radio communications" if "both the sender and all intended recipients are in the United States."[6] In 1978, almost all transoceanic communications into and out of the United States were radio communications carried by satellite. Accordingly, when FISA was enacted, the acquisition of most international communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition, discussed above); or (ii) *all* of the participants to the communication were located in the United States (in which case the acquisition would fall within the third definition).[7] Therefore, in 1978, if the government acquired communications by targeting a foreign person overseas, it usually was not engaged in "electronic surveillance"—a result consistent with Congress's expressed intent, discussed above, to carve out most overseas intelligence activities.

[5] 50 U.S.C. 1801(f)(1).
[6] 50 U.S.C. 1801(f)(1).
[7] 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.

It is important to note, however, that Congress created this carve-out by using the manner in which communications are transmitted as a proxy for the types of targets and communications that the statute intended to reach. As discussed below, this technology-dependent approach has had dramatic unintended consequences and has resulted in sweeping into FISA a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. And FISA's use of technology-dependent language is not limited to these core definitions of "electronic surveillance." The distinction between "wire" and "radio" communications runs throughout the statute, and the statute also contains a provision authorizing the acquisition of communications "transmitted by means of communications used exclusively between or among foreign powers" that was premised upon the telecommunications technologies of the 1970s.

In addition to reflecting the technology of the time, the Act's legislative history also shows that the world was a different place when FISA was enacted. In terms of civil liberties, one of Congress's primary concerns was preventing the improper collection and dissemination of information about Americans involved in the civil rights movement and political activities.[8] In terms of threats, Congress was, in large part, concerned with espionage by agents of the Soviet Union.[9] The United States had not yet confronted the perils of large-scale international terrorism within the homeland,[10] and the faces of terrorism were groups such as Black September, the Baader-Meinhof Group, and the Japanese Red Army.[11] It was a time when Congress was worried that, if a terrorist hijacked an airplane, the purpose would be "to force the government to release a certain class of prisoners or to suspend aid to a particular country"[12] – not murder 3,000

[8] *See, e.g.*, S. Rep. No. 95-701, at 19, 23, 26.
[9] *Id.* at 14.
[10] H.R. Rep. No. 95-1283, at 30.
[11] *Id.*
[12] *Id*. at 45; S. Rpt. 95-701, at 23-24.

innocent men, women, and children. Congress could not have foreseen international terrorism on a scale that amounts to armed conflict.

The FISA We Have Today: The Unintended Consequences of Technological Change

As this Committee is aware, there have been revolutions in telecommunications technology since 1978. For example, when FISA was enacted, almost all local calls were carried on a wire and almost all transoceanic communications were radio communications. Today that situation is almost precisely reversed, as most long-haul communications are on a wire and local calls often travel by air. And of course, today we have wholly new methods of communicating—such as cell phones and e-mail—that either did not exist or were not in popular use in 1978. The drafters of the FISA did not and could not have anticipated these developments.

These unanticipated advances in technology have wreaked havoc on the delicate balance that Congress originally struck when it enacted FISA. Most importantly, those advances have largely upended FISA's intended carve-out of intelligence activities directed at persons overseas. As a result, the scope of FISA has been expanded radically, without any conscious choice by the Congress, to encompass a wide range of activities that FISA did not cover in 1978.

While a thorough description of these consequences can be discussed only in a classified session, I can state the bottom line here: considerable resources of the Executive Branch and the FISA Court are now expended on obtaining court orders to monitor the communications of terrorist suspects overseas. I believe most Americans would be surprised and dismayed to discover that America's intelligence agencies routinely use scarce resources to make a showing of probable cause, a notion derived from the Fourth Amendment, and obtain a court order before

acquiring the communications of these individuals. To make matters worse, these individuals frequently are communicating with other persons outside the United States. In certain cases, this process of obtaining a court order slows, and in some cases may prevent, the Government's efforts to conduct surveillance of communications that are potentially vital to the national security.

This unintended expansion of FISA's scope has hampered our intelligence capabilities and has caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. This expansion of FISA's reach has necessarily diverted resources that would be better spent on protecting the privacy interests of United States persons here in the United States.

What We Should Do

We can and should amend FISA to restore its original focus on foreign intelligence activities that substantially implicate the privacy interests of individuals in the United States. The best way to restore that focus (and to reinstate the original carve-out for surveillance directed at foreign persons overseas) is to redefine the term "electronic surveillance" in a technology-neutral manner. Rather than focusing, as FISA does today, on *how* a communication travels or *where* it is intercepted, we should define FISA's scope by reference to *who is the subject of the surveillance*. If the surveillance is directed at a person in the United States, FISA generally should apply; if the surveillance is directed at persons overseas, it shouldn't. This would provide the Intelligence Community with much needed speed and agility while, at the

same time, refocusing FISA's privacy protections on United States persons located in the United States.

Some have suggested that the balance struck by Congress in 1978 did not go far enough; these critics argue that the Intelligence Community should be required to seek FISA Court approval each time a foreign target overseas happens to communicate with a person inside the United States. For reasons that I can elaborate upon in greater detail in closed session, this is an infeasible approach that would impose intolerable burdens on our intelligence efforts. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of such incidentally collected U.S. person information. 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.

In addition to this critical change in the definition of "electronic surveillance," the Administration's proposal—which draws from a number of thoughtful bills introduced in Congress during its last session—also would make several other salutary changes to FISA. While I explain these in greater detail below, I will briefly summarize a few of the core changes here. First, it would amend the statutory definition of "agent of a foreign power" – a category of individuals the government may target under FISA – to include any person other than a U.S. person who possesses or is expected to transmit or receive foreign intelligence information within the United States. Second, the bill would fill a gap in our laws by permitting the Government to direct communications companies to assist in the conduct of lawful communications intelligence activities that do not constitute "electronic surveillance" under

FISA, and ensuring that they are protected from liability for having assisted the government in its counterterrorism efforts. Third, the bill would 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. The other sections of the proposal, all of which are detailed below, work in concert with these provisions to ensure our security while preserving the civil liberties of Americans.

Before I explain each section of the proposal, I would like to address one other theme that has arisen regarding FISA modernization. Some have suggested that amending FISA is unnecessary, either because Congress has modified FISA several times since September 11th, or because they believe that increased resources could address any problems with the statute. Congress has acted wisely in making several changes to FISA that were necessary and which improved the security of our nation. However, to address our shared goal of detecting and preventing another terrorist attack, we submit that it also is necessary to update the framework governing foreign intelligence surveillance to reflect today's very different telecommunications technologies and threats. Likewise, although additional resources are always welcome, committing even substantial additional funds and other resources would not solve all of the problems posed by the current FISA framework. We should restore FISA to its original focus on establishing a framework for judicial approval of the interception of communications that substantially implicate the privacy interests of individuals in the United States; changes at the margins will not enable us to achieve this goal.

Section by Section Analysis

For purposes of providing a complete review of the proposed legislation, the following is a short summary of each proposed change in the bill – both major and minor.

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 of scenarios in which this gap is evident 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

For reasons that could not have been anticipated by Congress in 1978, FISA no longer reflects the delicate balance that Congress intended to strike when it enacted the statute. Radical technological changes in telecommunications have resulted in a vast array of overseas intelligence activities that were originally excluded from FISA being swept within FISA's scope. The proposal that the Administration has submitted to the Congress would restore FISA to its original focus on the protection of the privacy interests of Americans—a change that would both 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 privacy 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.