

March 12, 2008

The Honorable Nancy Pelosi  
Speaker  
United States House of Representatives  
Washington, DC 20511

Dear Madam Speaker:

We are deeply concerned about the impact of the House of Representative's latest proposal to modernize the Foreign Intelligence Surveillance Act of 1978 (FISA). The draft legislation unveiled just yesterday does not move us closer to resolving an issue that is critical to our ongoing efforts to protect the Nation. The proposal includes unworkable provisions, many of which we have addressed before, and includes new provisions drastically different from those in the bill that passed the Senate with wide bipartisan support. Some of these new provisions include:

- Requiring prior court approval to gather foreign intelligence from foreign targets located overseas. Congress did not include such a requirement when it passed the original FISA statute and with good reason—these foreign targets have no right to any court review of such surveillance under our Constitution. We know from experience that requiring prior court approval is a formula for delay. Thus, this framework would impede vital foreign intelligence collection and put the Nation at unnecessary and greater risk.
- Exposing intelligence operations conducted with the participation or assistance of a private individual or company—regardless whether they relate to FISA—to protracted litigation and disclosure in court proceedings. The proposal provides no relief from litigation imposed on those who are believed to have assisted the Government in the aftermath of September 11, 2001. Your proposal replaces the carefully considered bipartisan Senate provisions with an approach aimed at ensuring that litigation concerning highly classified programs will continue for years to come. In addition, the House proposal indicates that in any lawsuit against “any person for providing assistance to an element of the intelligence community,” the suit should go forward no matter the risk to vital sources and methods. Such a provision likely would severely hamper the ability of our intelligence community to gain private cooperation and make it difficult to protect national security information in litigation. In our view, even the status quo, which is degrading the Intelligence Community's ability to get cooperation from the private sector, would be preferable to this poorly conceived and deeply harmful proposal.
- Setting forth an unworkable “significant purpose” test to address a nonexistent problem. Such a test is directly at odds with the significant criticism of the Intelligence Community put forth by the congressional joint inquiry into September 11 and other reviews of intelligence operations. The purpose of our intelligence

operations is to protect the country from an attack. That includes detecting and acquiring a communication from terrorists abroad to operatives in this country—a communication that could be the final operational piece in an attack such as those being planned by our enemies at this moment. This provision has been rejected a number of times, including by a bipartisan majority in the Senate.

Because of these and other serious flaws in the bill that are outlined in detail below, we believe that this draft bill does not provide the Intelligence Community the tools it needs to collect effectively foreign intelligence information vital for the security of the Nation. If the President is sent a bill that does not provide the Intelligence Community the tools it needs to protect the country, the President will veto the bill.

Before turning to the specific problems with your proposal, it merits emphasizing a few points about the compromise Senate bill. After the passage of the Protect America Act last summer, the Senate immediately went to work, in a bipartisan fashion, to address two critical national security issues: First, how to maintain the core authorities provided by the Protect America Act, which authorized the Government to conduct surveillance of terrorists and other intelligence targets overseas without the need for individualized court approval, and second, how to provide just relief for private parties who have been sued solely because they are believed to have assisted the Government in responding to the catastrophic terrorist attacks on our country. The process in the Senate, which began in the Senate Intelligence Committee, was thoughtful and bipartisan and included the input of the Executive Branch's national security experts. It resulted in a bill that was adopted by a resounding 13 to 2 vote in the Intelligence Committee, and which then passed the Senate by a broad bipartisan vote of 68 to 29. This bill reflects significant compromises made by the Administration in an effort to accomplish objectives that are necessary to the national security; most notably, the bill for the first time would require the Government to obtain an order from the Foreign Intelligence Surveillance Court before targeting U.S. persons overseas. We believe this carefully crafted bipartisan compromise deserves consideration as it ensures the Intelligence Community has critical tools to carry out its operations while carefully protecting the rights of all Americans.

We do not believe that it is in the best interest of our national security to protract the process of modernizing FISA—a process which has been underway for years—any longer. We hope that the House can proceed in a manner that permits the bipartisan Senate compromise to come to a vote and places our intelligence operations on a stable foundation for the future.

\* \* \*

The most problematic provisions of the proposal are as follows:

Requires Prior Court Approval of Vital Foreign Intelligence Activities. The Protect America Act and the bipartisan Senate bill allow our intelligence professionals to target individuals abroad for surveillance without first going to a court. This approach is an appropriate framework in the context of foreign intelligence surveillance targeting foreign terrorists and other national security threats located outside the United States. Foreign targets have no right to court review of such surveillance under our Constitution, and it makes no sense to involve the court before the

Government begins surveillance of such targets who wish us harm. The new House bill, however, substantially increases the role of the court with respect to foreign intelligence targets located outside the United States. These provisions, which require prior court approval absent an emergency, would impede the collection of necessary foreign intelligence information and put the national security at risk without any meaningful increase in the protection of the privacy interests of Americans in the United States.

We have explained numerous times why prior court approval of surveillance targeting foreign terrorists and other national security threats located outside the United States impedes our intelligence collection and places the Nation at risk. Our foreign enemies seek to inflict catastrophic harm against Americans and our homeland; any delay in initiating surveillance of these foreign targets is unacceptable. The bill appears to require court action on the Government's request to initiate surveillance within thirty days, but a separate provision would allow for an extension of time on a very low standard. Thus, vital intelligence collection may well be delayed for months. Every day that surveillance is delayed, intelligence information is irretrievably lost. The Intelligence Community must be able to act with speed and agility to conduct surveillance of foreign terrorists and prevent attacks against our country. Prior court approval also would require intelligence analysts and others, before fulfilling their core duty—protecting the Nation—to prepare documents for court review. Initiating surveillance of individuals abroad without awaiting a court order—as the Senate bill provides—will ensure that we will keep closed the intelligence gaps that existed before the passage of the Protect America Act.

The provisions in the new House bill that allow the Government to begin surveillance in “emergency” situations are not an adequate substitute for the authority to initiate surveillance before obtaining court review. Given the catastrophic nature of the threats we face from foreign terrorists, the Government should not be forced to wait for an emergency to develop before it can take steps to gather information needed to prevent that emergency. Indeed, the job of the Intelligence Community is to obtain intelligence information that permits us to act before an emergency arises, and our intelligence professionals should be authorized to obtain foreign intelligence information in an expeditious and efficient manner. Moreover, given that what we wish to do is collect intelligence and not simply confirm knowledge that we already have, it may well be that we will not know when an emergency exists. Although the threats we face are catastrophic, not every threat would meet the “emergency” exception because many will not appear to be emergencies until it is too late. Prior court approval is appropriate when we target Americans in the United States where privacy concerns are directly implicated. It is not appropriate with respect to foreign targets outside the United States.

Imposes “the Significant Purpose” Test. The bill would prohibit acquisitions under the new authority if “the significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.” This provision is similar to provisions that were rejected in the Senate by bipartisan majorities. If the concern driving this proposal is so-called “reverse targeting”—circumstances in which the Government would conduct surveillance of a person overseas when the Government's actual target is a person in the United States with whom the person overseas is communicating—that situation is already addressed in FISA today. If the person in the United States is the actual

target, an order from the FISA Court is required. Indeed, section 703(b)(2) of the Senate bill codifies this longstanding Executive Branch interpretation of FISA.

The provision in the proposed House bill would place an unnecessary and debilitating burden on our Intelligence Community's ability to conduct surveillance without enhancing the protection of the privacy of Americans. The introduction of this ambiguous "significant purpose" standard would raise unacceptable operational uncertainties and problems, making it more difficult to collect intelligence when a foreign terrorist overseas is calling into the United States—which is precisely the communication we generally care most about. Part of the value of the Protect America Act, and the bipartisan Senate bill, is to enable the Intelligence Community to collect expeditiously the communications of terrorists in foreign countries who may contact an associate in the United States. In fact, the Intelligence Community was heavily criticized by numerous reviews after September 11, including by the Congressional Joint Inquiry into September 11, regarding its insufficient attention to detecting communications indicating homeland attack plotting. To quote the Congressional Joint Inquiry:

The Joint Inquiry has learned that one of the future hijackers communicated with a known terrorist facility in the Middle East while he was living in the United States. The Intelligence Community did not identify the domestic origin of those communications prior to September 11, 2001 so that additional FBI investigative efforts could be coordinated. Despite this country's substantial advantages, there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist-related communications, at least in terms of protecting the Homeland.

In addition, this poorly drafted provision would create uncertainty by focusing on whether the "significant purpose . . . is to acquire the communication" of a person in the United States, not just to target the person here. To be clear, a "significant purpose" of Intelligence Community activities that target individuals outside the United States is to detect communications that may provide warning of homeland attacks, including communications between a terrorist overseas and associates in the United States. A provision that bars the Intelligence Community from collecting these communications is flatly unacceptable.

**Fails to Provide Liability Protection to Private Sector Partners.** The new House bill fails to provide liability protection to companies that assisted the Government's efforts in the aftermath of the September 11th attacks to prevent another attack. Affording liability protection to those companies is a just result and is essential to ensuring that our Intelligence Community is able to carry out its mission. After reviewing the relevant documents, the Senate Intelligence Committee determined that providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. In its report on S. 2248, the Committee "concluded that the providers . . . had a good faith basis" for responding to the requests for assistance they received. The Senate Intelligence Committee ultimately agreed to necessary immunity protections on a nearly-unanimous, bipartisan, 13-2 vote, and the Senate passed its bill including liability protection by a 68-29 vote.

Providing this liability protection is critical to the national security. Companies that face lawsuits for allegedly assisting the Government may be unwilling to provide assistance if and when it is needed to prevent future terrorist attacks. As the Senate Intelligence Committee recognized, “the Intelligence Community cannot obtain the intelligence it needs without assistance from these companies.” That Committee also recognized that companies in the future may be less willing to assist the Government if they face the threat of private lawsuits each time they are alleged to have provided assistance. The Committee concluded that: “The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.” Senior intelligence officials also have testified regarding the importance of providing liability protection to such companies for these reasons.

Even prior to the expiration of the Protect America Act, we experienced significant difficulties in working with private sector companies because of the continued failure to provide liability protection for such companies. These difficulties have only grown since expiration of the Act without passage of the bipartisan Senate bill, which would provide fair and just liability protection. Exposing the private sector to the continued risk of multibillion-dollar class action suits for assisting in efforts to defend the country understandably makes company counsel much more reluctant to cooperate and much more inclined to litigate our requests for assistance—thereby delaying the surveillance we are requesting—in order to insulate their companies and shareholders from liability. Without their cooperation, our efforts to protect the country cannot succeed.

The liability protection offered in the bipartisan Senate bill applies only in a narrow set of circumstances. An action may be dismissed only if the Attorney General certifies to the court that either: (i) the electronic communications service provider did not provide the assistance; or (ii) the assistance was provided in the wake of the September 11th attacks, was designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States, and was described in a written request indicating that the activity was authorized by the President and determined to be lawful. A court must review this certification before an action may be dismissed. This immunity provision does not extend to the Government or Government officials, and it does not immunize any criminal conduct.

Affording liability protection to companies alleged to have assisted the Government in the aftermath of September 11, 2001, is critical to the national security, and we urge the House to pass the bipartisan liability protection provisions in the Senate bill.

**Prolonging Litigation Involving Sensitive National Security Information.** Instead of protecting extremely sensitive intelligence sources and methods by providing for the dismissal of litigation over alleged assistance provided to the Government in the aftermath of the September 11<sup>th</sup> attacks, the new House bill would replace the Senate’s bipartisan liability protections with the very process sought by the plaintiffs to continue the current litigation—a full examination in court and adjudication of allegations concerning classified intelligence activities that would require the disclosure of highly classified state secrets. Beyond the serious policy concerns discussed below, Title III of the bill also would raise grave constitutional questions about the authority of Congress to abrogate the President’s constitutional authority and responsibility to protect national security information. By allowing for the adjudication of claims pursuant to the

procedures set forth in section 106(f) of FISA, this provision makes it more likely that classified information will be disclosed. In short, in contrast to the Senate bill, the new House bill would not provide for the expeditious dismissal of the relevant litigation; it would instead likely result in protracted litigation that could go on for years. The companies being sued also would continue to be subjected to the burdens of the litigation and multibillion-dollar claims, and the continued litigation would increase the risk of the disclosure of highly classified information.

For no apparent reason, the House bill also would apply this framework well beyond the context of suits against telecommunications companies for allegedly assisting the Government in the aftermath of September 11, 2001. In contrast to the narrowly tailored liability protection provision in the bipartisan Senate bill, the provisions of Title III of the House bill would apply to any “suit in Federal or State court against any person for providing assistance to an element of the Intelligence Community.” Thus, it appears that the intent of Title III of the House bill is to abrogate the state secrets privilege and permit a merits adjudication of any case against a person for allegedly providing any assistance to the Intelligence Community. We hope that it was not your intent to place such a wide range of intelligence activities at risk of disclosure. Such a regime is unacceptable and has the potential to do catastrophic damage to our national security across a wide spectrum.

Applying section 106(f) of FISA in the cases covered by Title III of the new House bill, including the pending litigation, is inappropriate. Section 106(f) was designed for a much different circumstance—when the Government has already disclosed the existence of surveillance against a particular target—and it is a mechanism by which a claim challenging the acknowledged surveillance can be decided on the merits. Applying that mechanism broadly to cases against telecommunication companies, when the Government has not confirmed or denied whether particular companies have assisted with particular alleged activities (or even whether certain alleged activities exist), would force the dangerous disclosure of classified information in a way not contemplated under current section 106(f) cases. By undertaking a merits adjudication under section 106(f), a court would have to decide the validity of any claims and defenses and, therefore, whether or not the cases should proceed. Regardless of whether the court reviews the evidence *in camera* and *ex parte* in reaching its decision, the court’s ultimate decision would confirm or deny whether or not a specific company provided alleged assistance with respect to a particular alleged activity. As the Senate Intelligence Committee stated in its report, however, “the identities of persons or entities who provided assistance to the U.S. Government are protected as vital sources and methods of intelligence,” and it would be “inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance.”

In short, the House proposal is an ill-conceived and wholly unacceptable substitute for the carefully crafted liability protection contained in the bipartisan Senate bill. The proposal puts our intelligence operations at risk by discouraging the needed cooperation of our private partners and risking the disclosure of national security information.

Imposing a Short Sunset on the Legislation. The bill would shorten the existing sunset provision in the Senate bill from six years to less than twenty-two months. We strongly oppose this

provision. By its terms, this provision would withhold from our intelligence professionals the certainty and permanence they need to conduct foreign intelligence collection to protect Americans from terrorism and other threats to the national security. It is simply unworkable for the Intelligence Community to develop new processes and procedures and train their employees, only to have the law change within a short period of time. The threats we face do not come with an expiration date, and the fundamental rules governing our intelligence professionals' ability to track our enemies should not be in a persistent state of doubt. The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our adversaries are established and are not changing from year to year. Stability of law also allows the Intelligence Community and our private partners to invest resources appropriately.

Nor is there any need for a sunset. Congress has extensively debated and considered FISA modernization, and there is now a lengthy factual record on the need for this legislation. Administration officials have been working with Congress since at least the summer of 2006 on legislation to modernize FISA. Even prior to introduction of this new proposal in the House, Congress has held more than a dozen hearings and considered four versions of this bill, one out of each committee of jurisdiction in the House and the Senate, and 52 individual amendments. It has held 55 roll call votes in committee and on the floor of both houses. There also has been extensive congressional oversight and reporting regarding the Government's use of the authorities under the Protect America Act.

In addition, the Senate bill includes substantial congressional oversight of the Government's use of the authorities provided in the bill. This oversight includes provision of various written reports to the congressional intelligence committees, including semiannual assessments by the Attorney General and the Director of National Intelligence, assessments by each relevant agency's Inspector General, and annual reviews by the head of any agency conducting operations under Title VII of that bill. Congress can, of course, revisit these issues and amend a statute at whatever time it chooses. We therefore urge Congress to provide a long-term solution to an out-dated FISA and to resist attempts to impose a short expiration date on this legislation.

Creates a Commission on Surveillance Activities. The bill would establish a congressional commission to duplicate the extensive oversight performed by the congressional intelligence committees over the past two years. The proposed commission would also be charged with repeating much of the work already done by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), and the congressional Joint Inquiry into Intelligence Activities before and after the Terrorist Attacks of September 11, 2001. Unfortunately then, this proposal would do little more than retrace the well-trod ground of the past in an area that is already subject to extensive congressional oversight, rather than looking at how to keep our country safe in the future. The commission would be charged with "examining all programs and activities relating to intelligence collection inside the United States or regarding United States persons that were in effect or operation on September 11, 2001, and all such programs and activities undertaken since that date." This provision is unnecessary. The Executive Branch appropriately informs the congressional intelligence committees regarding

intelligence programs and activities, and those committees exercise ongoing oversight of those programs and activities. This oversight has included many hearings with Government and outside witnesses, extensive visits to review operations, nearly unprecedented access to documents related to the various intelligence activities, and responses to hundreds of questions for the record. The Intelligence Community and the Department of Justice have spent thousands of hours responding to congressional requests in this matter. Diverting operational personnel from their ongoing mission of protecting the country to cover ground already traversed is a poor use of limited resources. There is no reason to duplicate the work of the committees created by Congress to consider such matters. We also have serious concerns regarding the possible disclosure of highly classified information in the course of such a wide-ranging examination.

Eliminates the Carve-out of the Definition of “Electronic Surveillance”. The bill would eliminate section 701 of the Senate bill, which provides that nothing in the definition of “electronic surveillance” under FISA “shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States.” Section 701 of the Senate bill provides important clarity regarding the legal regime governing foreign intelligence surveillance, and that section should be retained. Without that carve-out, we are more likely to encounter difficulties in achieving private sector cooperation with activities authorized under the bill.

Acquisitions Involving United States Persons Outside the United States. The new House bill would amend some of the carefully crafted provisions in the Senate bill regarding the collection of intelligence involving U.S. persons outside the United States. These revisions would create significant ambiguities and operational problems. For example, the new House bill employs the phrase “communications information” in proposed section 703(a)(1). The use of that phrase would create unnecessary and troublesome ambiguities regarding the authorities set forth in that section. In addition, changes to the Senate proposal raise significant operational concerns with respect to the surveillance of U.S. person foreign intelligence targets abroad. The carefully crafted provisions in the Senate bill do not contain such flaws.

Fails to Include Procedures for Existing Statutory Defenses and Preemption of State Inquiries. The bill does not include the important provisions in the Senate bill that would establish procedures for implementing existing statutory defenses in the future and that would preempt state investigations of assistance provided by any electronic communication service provider to an element of the Intelligence Community. Those provisions are important to ensuring that electronic communication service providers can take full advantage of existing immunity provisions and to protecting highly classified information.

Imposes Court Review of Compliance with Minimization Procedures. The bill would allow the FISA Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information by targeting individuals reasonably believed to be outside the United States. This provision could place the FISA Court in a position where it would conduct individualized review of the Intelligence Community's foreign communications intelligence activities. Although conferring such authority on the court is understandable in the context of traditional FISA collection (which focuses on surveillances that most directly implicate the privacy of Americans), it is anomalous in this context, where the



court's role is in approving generally applicable procedures for collection targeting individuals outside the United States.

Includes an Expanded Exclusive Means Provision. The bill includes an unnecessary exclusive means provision; the Senate bill already addresses this issue. This provision would unduly complicate the ability of Congress to pass, in an emergency situation, a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Instead, it would require Congress to amend one of the specified provisions, which is much more complicated and time-consuming, or to enact specific statutory authorization for such activities. We believe that it is unwise to attempt to tie the hands of a future Congress in this manner. The inclusion of an exclusivity provision that goes beyond the one in the Senate bill raises a serious constitutional issue that does not need to be raised.

Inspector General Review of Terrorist Surveillance Program. The bill would require the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, and any other relevant element of the Intelligence Community to review certain surveillance activities, including the Terrorist Surveillance Program described by the President (TSP), conducted between September 11, 2001, and January 17, 2007. This provision is unnecessary. Various reviews by Inspectors General already are underway regarding the TSP. In addition, the congressional intelligence and judiciary committees, and much of the House and Senate leadership, have been briefed on the TSP. Moreover, certain congressional committees have conducted substantial oversight of these activities, which has included hearings with Government officials and outside parties concerning this program. It is wasteful and duplicative to require yet another inquiry into these issues.

We also are concerned with other flaws in the bill that would hamper the Intelligence Community's ability to collect the information necessary to protect the Nation.

\* \* \*

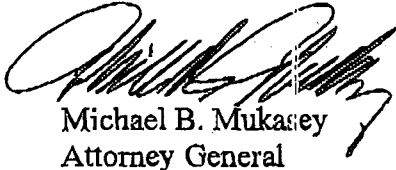
As we continue the process of modernizing FISA for the 21<sup>st</sup> century, it is important to remember that since September 11, 2001, we have been fighting a full-fledged war against international terrorists who are bent on inflicting maximum, and potentially catastrophic, damage against our citizens and our country. When we contemplate that stark reality, we are concerned that the House is considering legislation that would in some significant ways constitute a retreat and retrenchment of our national security authorities from those that were in place before September 11 and from the bipartisan Senate bill. With its imposition of a court order requirement that was never contemplated by the original FISA statute and its purported dismantling of much of the protection historically afforded by the state secrets doctrine in litigation over intelligence matters, the House proposal represents a significant step backward—at a time when we can least afford to compromise our intelligence capabilities.

We remain prepared to continue to work with Congress towards the passage of a long-term FISA modernization bill that would strengthen the Nation's intelligence capabilities while protecting the civil liberties of Americans, so that the President can sign such a bill into law. As we have explained before, the uncertainty caused by the failure to reauthorize the core authorities

The Honorable Nancy Pelosi  
Page 10 of 10

of the Protect America Act and to pass fair and just liability protection for the private sector continue to degrade our intelligence capabilities. We urge the House of Representatives to pass the bipartisan Senate bill as soon as possible.

Sincerely,



Michael B. Mukasey  
Attorney General



J.M. McConnell  
Director of National Intelligence