

February 5, 2008

The Honorable Harry Reid
Majority Leader
United States Senate
528 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Reid:

This letter presents the views of the Administration on various amendments to the Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008 (S. 2248), a bill "to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that act, and for other purposes." The letter also addresses why it is critical that the authorities contained in the Protect America Act not be allowed to expire. We have appreciated the willingness of Congress to address the need to modernize FISA and to work with the Administration to allow the intelligence community to collect the foreign intelligence information necessary to protect the Nation while protecting the civil liberties of Americans. We commend Congress for the comprehensive approach that it has taken in considering these authorities and are grateful for the opportunity to engage with Congress as it conducts an in-depth analysis of the relevant issues.

In August, Congress took an important step toward modernizing FISA by enacting the Protect America Act of 2007. That Act has allowed us temporarily to close intelligence gaps by enabling our intelligence professionals to collect, without a court order, foreign intelligence information from targets overseas. The intelligence community has implemented the Protect America Act in a responsible way, subject to extensive executive branch, congressional, and judicial oversight, to meet the country's foreign intelligence needs while protecting civil liberties. Indeed, the Foreign Intelligence Surveillance Court (FISA Court) recently approved the procedures used by the Government under the Protect America Act to determine that targets are located overseas, not in the United States.

The Protect America Act was scheduled to expire on February 1, 2008, but Congress has extended that Act for fifteen days, through February 16, 2008. In the face of the continued threats to our Nation from terrorists and other foreign intelligence targets, it is vital that Congress not allow the core authorities of the Protect America Act to expire, but instead pass long-term FISA modernization legislation that both includes the collection authority conferred by the Protect America Act and provides protection from private lawsuits against companies that are believed to have assisted the Government in the aftermath of the September 11th terrorist attacks on America. Liability protection is the just result for companies who answered their Government's call for assistance. Further, it will ensure that the Government can continue to rely upon the assistance of the private sector that is so necessary to protect the Nation and enforce its laws.

S. 2248, reported by the Senate Select Committee on Intelligence, would satisfy both of these imperatives. That bill was reported out of committee on a nearly unanimous 13-2 vote. Although it is not perfect, it contains many important provisions, and was developed through a thoughtful process that resulted in a bill that helps ensure that both the lives and the civil liberties of Americans will be safeguarded. First, it would establish a firm, long-term foundation for our intelligence community's efforts to track terrorists and other foreign intelligence targets located overseas. Second, S. 2248 would afford retroactive liability protection to communication service providers that are believed to have assisted the Government with intelligence activities in the aftermath of September 11th. In its report on S. 2248, the Intelligence Committee recognized that "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." The committee's measured judgment reflects the principle that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions. Thus, with the inclusion of the proposed manager's amendment, which would make necessary technical changes to the bill, we strongly support passage of S. 2248.

For reasons elaborated below, the Administration also strongly favors two other proposed amendments to the Intelligence Committee's bill. One would strengthen S. 2248 by expanding FISA to permit court-authorized surveillance of international proliferators of weapons of mass destruction. The other would ensure the timely resolution of any challenges to government directives issued in support of foreign intelligence collection efforts.

Certain other amendments have been offered to S. 2248, however, that would undermine significantly the core authorities and immunity provisions of that bill. After careful study, we have determined that those amendments would result in a final bill that would not provide the intelligence community with 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 U.S. intelligence agencies the tools they need to protect the nation, the President will veto the bill.

I. Limitations on the Collection of Foreign Intelligence

Several proposed amendments to S. 2248 would have a direct, adverse impact on our ability to collect effectively the foreign intelligence information necessary to protect the Nation. We note that three of these amendments were part of the Senate Judiciary Committee substitute, which has already been rejected by the Senate on a 60-34 vote. We explained why those three amendments were unacceptable in our November 14, 2007, letter to Senator Leahy regarding the Senate Judiciary Committee substitute, and the Administration reiterated these concerns in a Statement of Administration Policy (SAP) issued on December 17, 2007. A copy of that letter and the SAP are attached for your reference.

Prohibition on Collecting Vital Foreign Intelligence Information (No amendment number available). This amendment provides that "no communication shall be acquired under [Title VII of S. 2248] if the Government knows before or at the time of acquisition that the communication

is to or from a person reasonably believed to be located in the United States,” except as authorized under Title I of FISA or certain other exceptions. The amendment would require the Government to “segregate or specifically designate” any such communication and the Government could access such communications only under the authorities in Title I of FISA or under certain exceptions. Even for communications falling under one of the limited exceptions or an emergency exception, the Government still would be required to submit a request to the FISA Court relating to such communications. The procedural mechanisms it would establish would diminish our ability swiftly to monitor a communication from a terrorist overseas to a person in the United States—precisely the communication that the intelligence community may have to act on immediately. Finally, the amendment would draw unnecessary and harmful distinctions between types of foreign intelligence information, allowing the Government to collect communications under Title VII from or to the United States that contain information relating to terrorism but not other types of foreign intelligence information, such as that relating to the national defense of the United States or attacks, hostile actions, and clandestine intelligence activities of a foreign power.

This amendment would eviscerate critical core authorities of the Protect America Act and S. 2248. Our prior letter and the Statement of Administration Policy explained how this type of amendment increases the danger to the Nation and returns the intelligence community to a pre-September 11th posture that was heavily criticized in congressional reviews. It would have a devastating impact on foreign intelligence surveillance operations; it is unsound as a matter of policy; its provisions would be inordinately difficult to implement; and thus it is unacceptable. The incidental collection of U.S. person communications is not a new issue for the intelligence community. For decades, the intelligence community has utilized minimization procedures to ensure that U.S. person information is properly handled and “minimized.” It has never been the case that the mere fact that a person overseas happens to communicate with an American triggers a need for court approval. Indeed, if court approval were mandated in such circumstances, there would be grave operational consequences for the intelligence community’s efforts to collect foreign intelligence. Accordingly, if this amendment is part of the bill that is presented to the President, we, as well as the President’s other senior advisors, will recommend that he veto the bill.

Imposition of a “Significant Purpose” Test (No. 3913). This amendment, which was part of the Judiciary Committee substitute, would require an order from the Foreign Intelligence Surveillance Court (FISA Court) if a “significant purpose” of an acquisition targeting a person abroad is to acquire the communications of a specific person reasonably believed to be in the United States. 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, S. 2248 codifies this longstanding Executive Branch interpretation of FISA.

The amendment 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 any subsequent legislation, 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. 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, the proposed amendment 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 unacceptable. If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Imposition of a “Specific Individual Target” Test (No. 3912). This amendment, which was part of the Judiciary Committee substitute, would require the Attorney General and the Director of National Intelligence to certify that any acquisition “is limited to communications to which any party is a specific individual target (which shall not be limited to known or named individuals) who is reasonably believed to be located outside the United States.” This provision could hamper United States intelligence operations that currently are authorized to be conducted overseas and that could be conducted more effectively from the United States without harming the privacy interests of United States persons. For example, the intelligence community may wish to target all communications in a particular neighborhood abroad before our armed forces conduct an offensive. This amendment could prevent the intelligence community from targeting a particular group of buildings or a geographic area abroad to collect foreign intelligence prior to such military operations. This restriction could have serious consequences on our ability to collect necessary foreign intelligence information, including information vital to conducting military operations abroad and protecting the lives of our service members, and it is unacceptable. Imposing such additional requirements to the carefully crafted framework provided by S. 2248 would harm important intelligence operations without appreciably enhancing the privacy interests of Americans. If this amendment is part of the bill that is

presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Limits Dissemination of Foreign Intelligence Information (No. 3915). This amendment originally was offered in the Senate Intelligence Committee, where it was rejected on a 10-5 vote. The full Senate then rejected the amendment as part of its consideration of the Judiciary Committee amendment. The proposed amendment would impose significant new restrictions on the use of foreign intelligence information, including information not concerning United States persons, obtained or derived from acquisitions using targeting procedures that the FISA Court later found to be unsatisfactory for any reason. By requiring analysts to go back to the relevant databases and extract certain information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas. The effect of this burden would be to divert analysts and other resources from their core mission—protecting the Nation—to search for information, including information that does not concern United States persons. This requirement also stands at odds with the mandate of the September 11th Commission that the intelligence community should find and link disparate pieces of foreign intelligence information. Finally, the requirement would actually degrade—rather than enhance—privacy protections by requiring analysts to locate and examine United States person information that would otherwise not be reviewed. Accordingly, if this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

II. Liability Protection for Telecommunications Companies

Several amendments to S. 2248 would alter the carefully crafted provisions in that bill that afford liability protection to those companies believed to have assisted the Government in the aftermath of the September 11th attacks. Extending liability protection to such companies is imperative; failure to do so could limit future cooperation by such companies and put critical intelligence operations at risk. Moreover, litigation against companies believed to have assisted the Government risks the disclosure of highly classified information regarding extremely sensitive intelligence sources and methods. If any of these amendments is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Striking the Immunity Provisions (No. 3907). This amendment would strike Title II of S. 2248, which affords liability protection to telecommunications companies believed to have assisted the Government following the September 11th attacks. This amendment also would strike the important provisions in the 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.

Affording liability protection to those companies believed to have assisted the Government with communications intelligence activities in the aftermath of September 11th 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 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 Conference Report, 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. Twelve Members of the Committee subsequently rejected a motion to strike this provision.

The immunity offered in S. 2248 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, 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.

Providing this liability protection is critical to the national security. As the 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." Allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods. In addition to providing an advantage to our adversaries, the potential disclosure of classified information puts the facilities and personnel of electronic communication service providers at risk.

For these reasons, we, as well as the President's other senior advisors, will recommend that he veto any bill that does not afford liability protection to these companies.

Substituting the Government as the Defendant in Litigation (No. 3927). This amendment would substitute the United States as the party defendant for any covered civil action against a telecommunications provider if certain conditions are met. The Government would be substituted if the FISA Court determined that the company received a written request that complied with 18 U.S.C. § 2511(2)(a)(ii)(B), an existing statutory protection; the company acted in "good faith . . . pursuant to an objectively reasonable belief" that compliance with the written request was permitted by law; or that the company did not participate.

Substitution is not an acceptable alternative to immunity. Substituting the Government would simply continue the litigation at the expense of the American taxpayer. Substitution does nothing to reduce the risk of the further disclosure of highly classified information. The very point of these lawsuits is to prove plaintiffs' claims by disclosing classified information

regarding the activities alleged in the complaints, and this amendment would permit plaintiffs to participate in proceedings before the FISA Court regarding the conduct at issue. A judgment finding that a particular company is a Government partner also could result in the disclosure of highly classified information regarding intelligence sources and methods and hurt the company's reputation overseas. In addition, the companies would still face many of the burdens of litigation – including attorneys' fees and disruption to their businesses from discovery – because their conduct will be the key question in the litigation. Such litigation could deter private sector entities from providing assistance to the intelligence community in the future. Finally, the lawsuits could result in the expenditure of taxpayer resources, as the U.S. Treasury would be responsible for the payment of an adverse judgment. If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

FISA Court Involvement in Determining Immunity (No. 3919). This amendment would require all judges of the FISA Court to determine whether the written requests or directives from the Government complied with 18 U.S.C. § 2511(2)(a)(ii), an existing statutory protection; whether companies acted in “good faith reliance of the electronic communication service provider on the written request or directive under paragraph (1)(A)(ii), such that the electronic communication service provider had an objectively reasonable belief under the circumstances that the written request or directive was lawful”; or whether the companies did not participate in the alleged intelligence activities.

This amendment is not acceptable. It is for Congress, not the courts, to make the public policy decision whether to grant liability protection to telecommunications companies who are being sued simply because they are alleged to have assisted the Government in the aftermath of the September 11th attacks. The Senate Intelligence Committee has reviewed the relevant documents and concluded that those who assisted the Government acted in good faith and received written assurances that the activities were lawful and being conducted pursuant to a Presidential authorization. This amendment effectively sends a message of no-confidence to the companies who helped our Nation prevent terrorist attacks in the aftermath of the deadliest foreign attacks on U.S. soil. Transferring a policy decision critical to our national security to the FISA Court, which would be limited in its consideration to the particular matter before them (without any consideration of the impact of immunity on our national security), is unacceptable.

In contrast to S. 2248, this amendment would not allow for the expeditious dismissal of the relevant litigation. Rather, this amendment would do little more than transfer the existing litigation to the full FISA Court and would likely result in protracted litigation. The standards in the amendment also are ambiguous and would likely require fact-finding on the issue of good faith and whether the companies “had an objectively reasonable belief” that assisting the Government was lawful—even though the Senate Intelligence Committee has already studied this issue and concluded such companies did act in good faith. The companies being sued would continue to be subjected to the burdens of the litigation, and the continued litigation would increase the risk of the disclosure of highly classified information.

The procedures set forth under the amendment also present insurmountable problems. First, the amendment would permit plaintiffs to participate in the litigation before the FISA

Court. This poses a very serious risk of disclosure to plaintiffs of classified facts over which the Government has asserted the state secrets privilege and of disclosure of these secrets to the public. The FISA Court safeguards national security secrets precisely because the proceedings are generally *ex parte*—only the Government appears. The involvement of plaintiffs also is likely to prolong the litigation. Second, assembling the FISA Court for en banc hearings on these cases could cause delays in the disposition of the cases. Third, the amendment would purport to abrogate the state secrets privilege with respect to proceedings in the FISA Court. This would pose a serious risk of harm to the national security by possibly allowing plaintiffs access to highly classified information about sensitive intelligence activities, sources, and methods. The conclusion of the FISA Court also may reveal sensitive information to the public and our adversaries. Beyond these serious policy considerations, it also would raise very serious constitutional questions about the authority of Congress to abrogate the constitutionally-based privilege over national security information within the Executive's control. This is unnecessary, because classified information may be shared with a court *in camera* and *ex parte* even when the state secrets privilege is asserted. Fourth, the amendment does not explicitly provide for appeal of determinations by the FISA Court. Finally, imposing a standard involving an "objectively reasonable belief" is likely to cause companies in the future to feel compelled to make an independent finding prior to complying with a lawful Government request for assistance. Those companies do not have access to information necessary to make this judgment. Imposition of such a standard could cause dangerous delays in critical intelligence operations and put our national security at risk. As the Intelligence Committee recognized in its report on S. 2248, "the intelligence community cannot obtain the intelligence it needs without assistance from these companies." For these reasons, existing law rightly places no such obligation on telecommunications companies.

If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

III. Other Amendments

Imposing a Short Sunset on the Legislation (No. 3930). This amendment would shorten the existing sunset provision in S. 2248 from six years to four years. We strongly oppose it. S. 2248 should not have an expiration date at all. The threats we face do not come with an expiration date, and our authorities to counter those threats should be placed on a permanent foundation. They should not be in a continual state of doubt. Any sunset provision withholds from our intelligence professionals and our private partners the certainty and permanence they need to protect Americans from terrorism and other threats to the national security. 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. There has been extensive public discussion, debate, and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation. Indeed, Administration officials have been working with Congress since at least the summer of 2006 on legislation to modernize FISA. There also has been extensive congressional oversight and reporting regarding the Government's use of the authorities under the Protect America Act. In addition, S. 2248 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. 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. Although we believe that any sunset is unwise and unnecessary, we support S. 2248 despite its six-year sunset because it meets our operational needs to keep the country safe by providing needed authorities and liability protection.

Imposes Court Review of Compliance with Minimization Procedures (No. 3920). This amendment, which was part of the Judiciary Committee substitute, 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. We strongly oppose this amendment. It could place the FISA Court in a position where it would conduct individualized review of the intelligence community's foreign communications intelligence activities. While conferring such authority on the court is understandable in the context of traditional FISA collection, 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.

Congress is aware of the substantial oversight of the use of the authorities contained in the Protect America Act. As noted above, S. 2248 significantly increases such oversight by mandating 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, as well as extensive reporting to Congress and to the FISA Court. The repeated layering of overlapping oversight requirements on one aspect of intelligence community operations is both unnecessary and not the best use of limited resources and expertise.

Expedited FISA Court Review of Challenges and Petitions to Compel Compliance (No. 3941). This amendment would require the FISA Court to make an initial ruling on the frivolousness of a challenge to a directive issued under the bill within five days, and to review any challenge that requires plenary review within 30 days. The amendment also provides that if the Constitution requires it, the court can take longer to decide the issues before it. The amendment sets forth similar procedures for the enforcement of directives (*i.e.*, when the Government seeks to compel an electronic communication service provider to furnish assistance or information). This amendment would ensure that challenges to directives and petitions to compel compliance with directives are adjudicated in a manner that avoids undue delays in critical intelligence collection. This amendment would improve the existing provisions in S. 2248 pertaining to challenges to directives and petitions to compel cooperation by electronic communication service providers, and we strongly support it.

Proliferation of Weapons of Mass Destruction (No. 3938). This amendment, which would apply to surveillance pursuant to traditional FISA Court orders, would expand the definition of

“foreign power” to include groups engaged in the international proliferation of weapons of mass destruction. This amendment reflects the threat posed by these catastrophic weapons and extends FISA to apply to individuals and groups engaged in the international proliferation of such weapons. To the extent that they are not also engaged in international terrorism, FISA currently does not cover those engaged in the international proliferation of weapons of mass destruction. The amendment would expand the definition of “agent of a foreign power” to include non-U.S. persons engaged in such activities, even if they cannot be connected to a foreign power before the surveillance is initiated. The amendment would close an existing gap in FISA’s coverage with respect to surveillance conducted pursuant to traditional FISA Court orders, and we strongly support it.

Exclusive Means (No. 3910). We understand that the amendment relating to the exclusive means provision in S. 2248 is undergoing additional revision. As a result, we are withholding comment on this amendment and its text at this time. We note, however, that we support the provision currently contained in S. 2248 and to support its modification, we would have to conclude that the amendment provides for sufficient flexibility to permit the President to protect the Nation adequately in times of national emergency.

IV. Expiration

While it is essential that any FISA modernization presented to the President provide the intelligence community with the tools it needs while safeguarding the civil liberties of Americans, it is also vital that Congress not permit the authorities of the Protect America Act not be allowed simply to expire. As you are aware, the Protect America Act, which allowed us temporarily to close gaps in our intelligence collection, was to sunset on February 1, 2008. Because Congress indicated that it was “a legislative impossibility” to meet this deadline, it passed and the President signed a fifteen-day extension. Failure to pass long-term legislation during this period would degrade our ability to obtain vital foreign intelligence information, including the location, intentions, and capabilities of terrorists and other foreign intelligence targets abroad.

First, the expiration of the authorities in the Protect America Act would plunge critical intelligence programs into a state of uncertainty which could cause us to delay the gathering of, or simply miss, critical foreign intelligence information. Expiration would result in a degradation of critical tools necessary to carry out our national security mission. Without these authorities, there is significant doubt surrounding the future of aspects of our operations. For instance, expiration would create uncertainty concerning:

- The ability to modify certifications and procedures issued under the Protect America Act to reflect operational needs and the implementation of procedures to ensure that agencies are fully integrated protecting the Nation;
- The continuing validity of liability protection for those who assist us according to the procedures under the Protect America Act;
- The continuing validity of the judicial mechanism for compelling the assistance needed to protect our national security;

- The ability to cover intelligence gaps created by new communication paths or technologies. If the intelligence community uncovers such new methods, it will need to act to cover these intelligence gaps.

All of these aspects of our operations are subject to great uncertainty and delay if the authorities of the Protect America Act expire. Indeed, some critical operations will likely not be possible without the tools provided by the Protect America Act. We will be forced to pursue intelligence collection under FISA's outdated legal framework—a framework that we already know leads to intelligence gaps. This degradation of our intelligence capability will occur despite the fact that, as the Department of Justice has notified Congress, the FISA Court has approved our targeting procedures pursuant to the Protect America Act.

Second, expiration or continued short-term extensions of the Protect America Act means that an issue of paramount importance will not be addressed. This is the issue of providing liability protection for those who provided vital assistance to the Nation after September 11, 2001. Senior leaders of the intelligence community have consistently emphasized the critical need to address this issue since 2006. *See*, "FISA for the 21st Century" hearing before the Senate Judiciary Committee with Director of the Central Intelligence Agency and Director of the National Security Agency; 2007 Annual Threat Assessment Hearing before the Senate Select Committee on Intelligence with Director of National Intelligence. Ever since the first Administration proposal to modernize FISA in April 2007, the Administration had noted that meeting the intelligence community's operational needs had two critical components—modernizing FISA's authorities and providing liability protection. The Protect America Act updated FISA's legal framework, but it did not address the need for liability protection.

As we have discussed above, and the Senate Intelligence Committee recognized, "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation." As it concluded, "[t]he possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." In short, if the absence of retroactive liability protection leads to private partners not cooperating with foreign intelligence activities, we can expect more intelligence gaps.

Questions surrounding the legality of the Government's request for assistance following September 11th should not be resolved in the context of suits against private parties. By granting responsible liability protection, S. 2248 "simply recognizes that, in the specific historical circumstances here, if the private sector relied on written representations that high-level Government officials had assessed the [the President's] program to be legal, they acted in good faith and should be entitled to protection from civil suit." Likewise, we do not believe that it is constructive—indeed, it is destructive—to degrade the ability of the intelligence community to protect the country by punishing our private partners who are not part of the ongoing debate between the branches over their respective powers.

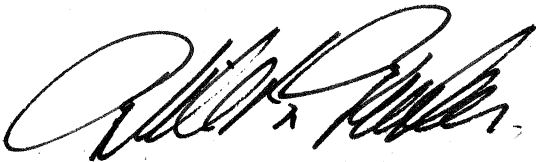
* * * * *

The Honorable Harry Reid

The Protect America Act's authorities expire in less than two weeks. The Administration remains prepared to work with Congress towards the passage of a FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting and protecting the constitutional rights of Americans, so that the President can sign such a bill into law. Passage of S. 2248 and rejection of those amendments that would undermine it would be a critical step in this direction. We look forward to continuing to work with you and the Members of the Senate on these important issues.

Thank you for the opportunity to present our views. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of this letter.

Sincerely,



Michael B. Mukasey
Attorney General



J.M. McConnell
Director of National Intelligence

cc: The Honorable Mitch McConnell
Minority Leader
The Honorable Patrick Leahy
Chairman, Committee on the Judiciary
The Honorable Arlen Specter
Ranking Minority Member, Committee on the Judiciary
The Honorable John D. Rockefeller
Chairman, Select Committee on Intelligence
The Honorable Christopher S. Bond
Vice Chairman, Select Committee on Intelligence

Attachments