

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

The Honorable Harry Reid

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

The Honorable Harry Reid

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

November 14, 2007

**The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510**

Dear Mr. Chairman:

This letter presents the views of the Administration on the proposed substitute amendment you circulated to Title I of the FISA Amendments Act of 2007 (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." We have appreciated the willingness of Congress to address the need to modernize FISA permanently and to work with the Administration to do so in a manner that allows the intelligence community to collect the foreign intelligence information necessary to protect the Nation while protecting the civil liberties of Americans. With all respect, however, we strongly oppose the proposed substitute amendment. If the substitute is part of a bill that is presented to the President, we and the President's other senior advisers will recommend that he veto the bill.

In August, Congress took an important step toward modernizing the Foreign Intelligence Surveillance Act of 1978 by enacting the Protect America Act of 2007 (PAA). The Protect America 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 congressional oversight, to meet the country's foreign intelligence needs while protecting civil liberties. Unless reauthorized by Congress, however, the authority provided in the Protect America Act will expire in less than three months. In the face of the continued terrorist threats to our Nation, we think it is vital that Congress act to make the core authorities of the Protect America Act permanent. Congressional action to provide protection from private lawsuits against companies that are alleged to have assisted the Government in the aftermath of the September 11th terrorist attacks on America also is critical to ensuring the Government can continue to receive private sector help to protect the Nation.

In late October, the Senate Select Committee on Intelligence introduced a consensus, bipartisan bill (S. 2248) that would establish a firm, long-term foundation for our intelligence community's efforts to target terrorists and other foreign intelligence targets located overseas. While the bill is not perfect, it contains many important provisions, and was developed through a thoughtful process that ensured that the intelligence community retains the core authorities it needs to protect the Nation and that the bill would not adversely impact critical intelligence operations. Importantly, that bill would afford retroactive liability protection to communication service providers that are alleged to have assisted the Government with intelligence activities in the aftermath of September 11th. 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. The bill was reported favorably out of committee on a 13-2 vote.

We respectfully submit that your substitute amendment to Title I of the Senate Intelligence Committee’s bill would upset some important provisions in the Intelligence Committee bill. The substitute also does not adequately address certain provisions in the Intelligence Committee’s bill that remain in need of improvement. As a result, we have determined, with all respect to your efforts, that the substitute would not provide the intelligence community with the tools it needs effectively to collect foreign intelligence information vital for the security of the Nation.

I. Limitations on Intelligence Collection and National Security Investigations

The substitute would make several amendments to S. 2248 that would have an adverse impact on our ability to collect effectively the foreign intelligence information necessary to protect the Nation. These amendments include the following:

Prohibits Intelligence and Law Enforcement Officials From Using Valuable Investigative Tools. The substitute contains an amendment to the “exclusive means” provision of FISA that could severely harm our ability to conduct national security investigations. As drafted, the provision would bar the use of national security letters, Title III criminal wiretaps, and other well-established investigative tools to collect information in national security investigations.

Threatens Critical Intelligence Collection Activities. The “exclusive means” provision also could harm the national security by disrupting highly classified intelligence activities. Among other things, ambiguities in critical terms and formulations in the provision—including the term “communications information” (a term that is not defined in FISA) and the introduction of the concept of targeting communications (as opposed to persons)—could lead the statute to bar altogether or to require court approval for overseas intelligence activities that involve merely the incidental collection of United States person information.

Limits Existing Provisions of Law that Protect Communications Service Providers. The portion of the substitute regarding protections to communication service providers under Government certifications contains ambiguities that could jeopardize our ability to secure the assistance of these providers in the future. This could hamper significantly the Government’s efforts to obtain necessary foreign intelligence information. As the Senate Intelligence Committee noted in its report on S. 2248, “electronic communications service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies.”

Allows for Dangerous Intelligence Gaps During the Pendency of an Appeal. The substitute would delete an important provision in the bipartisan Intelligence Committee bill that would ensure that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA Court. Without that provision, whole categories of surveillances directed outside the United States could be halted before review by the FISA Court of Review.

Limits Dissemination of Foreign Intelligence Information. The substitute 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. By requiring analysts to go back to the databases and pull out the 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. This requirement also strikes us as at odds with the mandate of the September 11th Commission that the intelligence community should find and link disparate pieces of foreign intelligence information. The requirement also harms privacy interests by requiring analysts to examine information that would otherwise be discarded without being reviewed.

Imposes Court Review of Compliance with Minimization Procedures. The 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. This 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 rather than individual surveillances.

Strikes a Provision Designed to Make the FISA Process More Efficient. The substitute would strike a provision from the bipartisan Senate Intelligence Committee bill that would allow the second highest-ranking FBI official to certify applications for electronic surveillance. Today, the only FBI official who can certify FISA applications is the Director, a restriction that can delay the initiation of surveillance when the Director travels or is otherwise unavailable. It is unclear why this provision from the Intelligence Committee bill, which will enhance the efficiency of the FISA process while ensuring high-level accountability, would be objectionable.

II. Necessary Improvements to S. 2248

The substitute also does not make needed improvements to the Senate Intelligence Committee bill. These include:

Provision Pertaining to Surveillance of United States Persons Abroad. The substitute does not make needed improvements to the Committee bill, which would require for the first time that a court order be obtained to surveil United States persons abroad. In addition to being problematic for policy reasons and imposing burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes, the provision continues to have serious technical problems. As drafted, the provision would not allow for the surveillance, even with a court finding, of certain critical foreign intelligence targets, and would allow emergency surveillance outside the United States for significantly less time than the bipartisan Senate Intelligence Committee bill had authorized for surveillance inside the United States.

Maintains a Sunset Provision. Rather than achieving permanent FISA reform, the substitute maintains a six year sunset provision. Indeed, several members on the Judiciary Committee have indicated that they may propose amendments to the bill that would shorten the sunset, leaving the intelligence community and our private partners subject to an uncertain legal framework for collecting intelligence from overseas targets. Any sunset provision withholds 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. 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, we submit, also allows the intelligence community to invest resources appropriately. In our respectful view, a sunset provision is unnecessary and would have an adverse impact on the intelligence community's ability to conduct its mission efficiently and effectively.

Fails to Remedy an Unrealistic Reporting Requirement. The substitute fails to make needed amendments to a reporting requirement in the Senate Intelligence Committee bill that poses serious operational difficulties for the intelligence community. The Intelligence Committee bill contains a requirement that intelligence analysts count "the number of persons located in the United States whose communications were reviewed." This provision would be impossible to implement fully. The provision, in short, places potentially insurmountable burdens on intelligence professionals without meaningfully protecting the privacy of Americans. The intelligence community has provided Congress with a further classified discussion of this issue.

We also are concerned by other serious technical flaws in the substitute that create uncertainty.

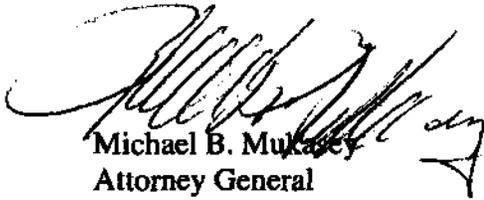
The Administration remains prepared to work with Congress towards the passage of a permanent FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting and protecting the constitutional rights of Americans, so that the President can sign such a bill into law. We look forward to working with you and the Members of the Judiciary Committee on these important issues.

Thank you for the opportunity to present our views. The Office of Management and

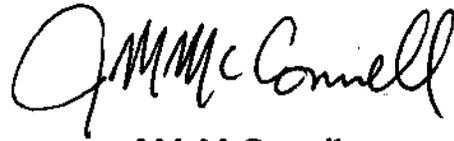
The Honorable Patrick J. Leahy
Page 5

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 Arlen Specter
Ranking Minority Member
The Honorable John D. Rockefeller
Chairman, Select Committee on Intelligence
The Honorable Christopher S. Bond
Vice Chairman, Select Committee on Intelligence



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

December 17, 2007
(Senate)

STATEMENT OF ADMINISTRATION POLICY

S. 2248 – To amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that act, and for other purposes

(Sen. Rockefeller (D) WV)

Protection of the American people and American interests at home and abroad requires access to timely, accurate, and insightful intelligence on the capabilities, intentions, and activities of foreign powers, including terrorists. The Protect America Act of 2007 (PAA), which amended the Foreign Intelligence Surveillance Act of 1978 (FISA) this past August, has greatly improved the Intelligence Community's ability to protect the Nation from terrorist attacks and other national security threats. The PAA has allowed us to close intelligence gaps, and it has enabled our intelligence professionals to collect foreign intelligence information from targets overseas more efficiently and effectively. The Intelligence Community has implemented the PAA under a robust oversight regime that has protected the civil liberties and privacy rights of Americans. Unfortunately, the benefits conferred by the PAA are only temporary because the act sunsets on February 1, 2008.

The Director of National Intelligence has frequently discussed what the Intelligence Community needs in permanent FISA legislation, including two key principles. First, judicial authorization should not be required to gather foreign intelligence from targets located in foreign countries. Second, the law must provide liability protection for the private sector.

The Senate is considering two bills to extend the core authorities provided by the PAA and modernize FISA. In October, the Senate Select Committee on Intelligence (SSCI) passed a consensus, bipartisan bill (S. 2248) that would establish a sound foundation for our Intelligence Community's efforts to target terrorists and other foreign intelligence targets located overseas. Although the bill is not perfect and its flaws must be addressed, it nevertheless represents a bipartisan compromise that will ensure that the Intelligence Community retains the authorities it needs to protect the Nation. Indeed, the SSCI bill is an improvement over the PAA in one essential way—it would provide retroactive liability protection to electronic communication service providers that are alleged to have assisted the Government with intelligence activities in the aftermath of September 11th.

In sharp contrast to the SSCI's bipartisan approach to modernizing FISA, the Senate Judiciary Committee reported an amendment to the SSCI bill that would have devastating consequences to the Intelligence Community's ability to detect and prevent terrorist attacks and to protect the Nation from other national security threats. The Judiciary Committee proposal would degrade our foreign intelligence collection capabilities. The Judiciary Committee's amendment would impose unacceptable and potentially crippling burdens on the collection of foreign intelligence information by expanding FISA to restrict facets of foreign intelligence collection never intended

to be covered under the statute. Furthermore, the Judiciary Committee amendment altogether fails to address the critical issue of liability protection. Accordingly, if the Judiciary Committee's substitute amendment is part of a bill that is presented to the President, the Director of National Intelligence, the Attorney General, and the President's other senior advisors will recommend that he veto the bill.

The Senate Select Committee on Intelligence Bill

Building on the authorities and oversight protections included in the PAA, the SSCI drafted S. 2248 to provide a sound legal framework for essential foreign intelligence collection in a manner consistent with the Fourth Amendment. As in the PAA, S. 2248 permits the targeting of foreign terrorists and other foreign intelligence targets outside the United States based upon the approval of the Director of National Intelligence and the Attorney General.

The SSCI drafted its bill in extensive coordination with Intelligence Community and national security professionals—those who are most familiar with the needs of the Intelligence Community and the complexities of our intelligence laws. The SSCI also heard testimony from privacy experts in order to craft a balanced approach. As a result, the SSCI bill recognizes the importance of clarity in laws governing intelligence operations. Although the Administration would strongly prefer that the provisions of the PAA be made permanent without modification, the Administration engaged in extensive consultation in the interest of achieving permanent legislation in a bipartisan manner.

The SSCI bill is not perfect, however. Indeed, certain provisions represent a major modification of the PAA and will create additional burdens for the Intelligence Community, including by dramatically expanding the role of the FISA Court in reviewing foreign intelligence operations targeted at persons located *outside* the United States, a role never envisioned when Congress created the FISA court.

In particular, the SSCI bill contains two provisions that must be modified in order to avoid significant negative impacts on intelligence operations. Both of these provisions are also included in the Judiciary Committee substitute, detailed further below.

First, as part of the debate over FISA modernization, concerns have been raised regarding acquiring information from U.S. persons outside the United States. Accordingly, the SSCI bill provides for FISA Court approval of surveillance of U.S. persons abroad. The Administration opposes this provision. Under executive orders in place since before the enactment of FISA in 1978, Attorney General approval is required before foreign intelligence surveillance and searches may be conducted against a U.S. person abroad under circumstances in which a person has a reasonable expectation of privacy. More specifically, section 2.5 of Executive Order 12333 requires that the Attorney General find probable cause that the U.S. person target is a foreign power or an agent of a foreign power. S. 2248 dramatically increases the role of the FISA Court by requiring court approval of this probable cause determination before an intelligence operation may be conducted beyond the borders of the United States. This provision imposes burdens on foreign intelligence collection abroad that frequently do not exist even with respect to searches and surveillance abroad for law enforcement purposes. Were the Administration to consider accepting FISA Court approval for foreign intelligence searches and surveillance of U.S. persons overseas, technical corrections would be necessary. The

Administration appreciates the efforts that have been made by Congress to address these issues, but notes that while it may be willing to accept that the FISA Court, rather than the Attorney General, must make the required findings, limitations on the scope of the collection currently allowed are unacceptable.

Second, the Senate Intelligence Committee bill contains a requirement that intelligence analysts count “the number of persons located in the United States whose communications were reviewed.” This provision would likely be impossible to implement. It places potentially insurmountable burdens on intelligence professionals without meaningfully protecting the privacy of Americans, and takes scarce analytic resources away from protecting our country. The Intelligence Community has provided Congress with a detailed classified explanation of this problem.

Although the Administration believes that the PAA achieved foreign intelligence objectives with reasonable and robust oversight protections, S.2248, as drafted by the Senate Intelligence Committee, provides a workable alternative and improves on the PAA in one critical respect by providing retroactive liability protection. The Senate Intelligence Committee bill would achieve an effective legislative result by returning FISA to its appropriate focus on the protection of privacy interests of persons inside the United States, while retaining our improved capability under PAA to collect timely foreign intelligence information needed to protect the Nation.

The Senate Judiciary Committee Proposal

The Senate Judiciary Committee amendment contains a number of provisions that would have a devastating impact on our foreign intelligence operations.

Among the provisions of greatest concern are:

An Overbroad Exclusive Means Provision That Threatens Worldwide Foreign Intelligence Operations. Consistent with current law, the exclusive means provision in the SSCI’s bill addresses only “electronic surveillance” and “the interception of domestic wire, oral, and electronic communications.” But the exclusive means provision in the Judiciary Committee substitute goes much further and would dramatically expand the scope of activities covered by that provision. The Judiciary Committee substitute makes FISA the exclusive means for acquiring “communications information” for foreign intelligence purposes. The term “communications information” is not defined and potentially covers a vast array of information—and effectively bars the acquisition of much of this information that is currently authorized under other statutes such as the National Security Act of 1947, as amended. It is unprecedented to require specific statutory authorization for every activity undertaken worldwide by the Intelligence Community. In addition, the exclusivity provision in the Judiciary Committee substitute ignores FISA’s complexity and its interrelationship with other federal laws and, as a result, could operate to preclude the Intelligence Community from using current tools and authorities, or preclude Congress from acting quickly to give the Intelligence Community the tools it may need in the aftermath of a terrorist attack in the United States or in response to a grave threat to the national security. In short, the Judiciary Committee’s exclusive means provision would radically reshape the intelligence collection framework and is unacceptable.

Limits on Foreign Intelligence Collection. The Judiciary Committee substitute would require the Attorney General and the Director of National Intelligence to certify for certain acquisitions that they are “limited to communications to which at least one party is a specific individual target who is reasonably believed to be located outside the United States.” This provision is unacceptable because it could hamper U.S. intelligence operations that are currently authorized to be conducted overseas and that could be conducted more effectively from the United States without harming U.S. privacy rights.

Significant Purpose Requirement. The Judiciary Committee substitute would require a FISA court order 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 target, a significant purpose of the acquisition must be to collect foreign intelligence information, and an order from the FISA court is required. Indeed, the SSCI bill codifies this longstanding Executive Branch interpretation of FISA. The Judiciary Committee substitute 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.

Part of the value of the PAA, 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.

(S. Rept. No. 107-351, H. Rept. No. 107-792 at 36.) To be clear, a “significant purpose” of Intelligence Community activities is to detect communications that may provide warning of homeland attacks and that may include communication between a terrorist overseas who places a call to associates in the United States. A provision that bars the Intelligence Community from collecting these communications is unacceptable, as Congress has stated previously

Liability Protection. In contrast to the Senate Intelligence Committee bill, the Senate Judiciary Committee substitute would not protect electronic communication service providers who are alleged to have assisted the Government with communications intelligence activities in the aftermath of September 11th from potentially debilitating lawsuits. Providing liability protection to these companies is a just result. In its Conference Report, the Senate Intelligence Committee “concluded that the providers . . . had a good faith basis for responding to the requests for

assistance they received.” The Committee further recognized that “the Intelligence Community cannot obtain the intelligence it needs without assistance from these companies.” 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 Senate Intelligence 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 by revealing sources and methods during the course of litigation, the potential disclosure of classified information puts both the facilities and personnel of electronic communication service providers and our country’s continued ability to protect our homeland at risk. It is imperative that Congress provide liability protection to those who cooperated with this country in its hour of need.

The ramifications of the Judiciary Committee’s decision to afford no relief to private parties that cooperated in good faith with the U.S. Government in the immediate aftermath of the attacks of September 11 could extend well beyond the particular issues and activities that have been of primary interest and concern to the Committee. The Intelligence Community, as well as law enforcement and homeland security agencies, continue to rely on the voluntary cooperation and assistance of private parties. A decision by the Senate to abandon those who may have provided assistance after September 11 will invariably be noted by those who may someday be called upon again to help the Nation.

Mandates an Unnecessary Review of Historical Programs. The Judiciary Committee substitute would require that inspectors general of the Department of Justice and relevant Intelligence Community agencies audit the Terrorist Surveillance Program and “any closely related intelligence activities.” If this “audit” is intended to look at operational activities, there has been an ongoing oversight activity by the Inspector General of the National Security Agency (NSA) of operational activities and the Senate Intelligence Committee has that material. Mandating a new and undefined “audit” will divert significant operational resources from current issues to redoing past audits. The Administration understands, however, the “audit” may in fact not be related to technical NSA operations. If it is the case that in fact the Judiciary Committee is interested in historical reviews of legal issues, the provision is unnecessary. The Department of Justice Inspector General and the Office of Professional Responsibility are already doing a comprehensive review. In addition, the phrase “closely related intelligence activities” would introduce substantial ambiguities in the scope of this review. Finally, this provision would require the inspectors general to acquire “all documents relevant to such programs” and submit those documents with its report to the congressional intelligence and judiciary committees. The requirement to collect and disseminate this wide range of highly classified documents—including all those “relevant” to activities “closely related” to the Terrorist Surveillance Program—unnecessarily risks the disclosure of extremely sensitive information about our intelligence activities, as does the audit requirement itself. Taking such national security risks for a backwards-looking purpose is unacceptable.

Allows for Dangerous Intelligence Gaps During the Pendency of an Appeal. The Judiciary Committee substitute would delete an important provision in the SSCI bill that enables the Intelligence Community to collect foreign intelligence from overseas terrorists and other foreign intelligence targets during an appeal. Without that provision, we could lose vital intelligence necessary to protect the Nation because of the views of one judge.

Limits Dissemination of Foreign Intelligence Information. The Judiciary Committee substitute 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 databases and pull out certain information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, burden on the Intelligence Community. Moreover, this provision would degrade privacy protections, as it would require analysts to locate and examine U.S. person information that would otherwise not be reviewed.

Requires FISA Court Approval of All “Targeting” for Foreign Intelligence Purposes. The Judiciary Committee substitute potentially requires the FISA Court to approve “[a]ny targeting of persons reasonably believed to be located outside the United States.” Although we assume that the Committee did not intend to require these procedures to govern all “targeting” done of any person in the world for any purpose—whether it is to gather human intelligence, communications intelligence, or for other reasons—the text as passed by the Committee contains no limitation. Such a requirement would bring within the FISA Court a vast range of overseas intelligence activities with little or no connection to civil liberties and privacy rights of Americans.

Imposes Court Review of Compliance with Minimization Procedures. The Judiciary Committee substitute would require the FISA Court to review and assess compliance with minimization procedures. Together with provisions discussed above, this would constitute a massive expansion of the Court’s role in overseeing the Intelligence Community’s implementation of foreign intelligence collection abroad.

Amends FISA to Impose Burdensome Document Production Requirements. The Judiciary Committee substitute would amend FISA to require the Government to submit to oversight committees a copy of any decision, order, or opinion issued by the FISA Court or the FISA Court of Review that includes significant construction or interpretation of any provision of FISA, including any pleadings associated with those documents, no later than 45 days after the document is issued. The Judiciary Committee substitute also would require the Government to retrieve historical documents of this nature from the last five years. As drafted, this provision could impose significant burdens on Department of Justice staff assigned to support national security operational and oversight missions.

Includes an Even Shorter Sunset Provision Than That Contained in the SSCI Bill. The Judiciary Committee substitute and the SSCI bill share the same flaw of failing to achieve permanent FISA reform. The Judiciary Committee substitute worsens this flaw, however, by shortening the sunset provision in the SSCI bill from six years to four years. Any sunset provision, but particularly one as short as contemplated in the Judiciary Committee substitute, would adversely impact the Intelligence Community’s ability to conduct its mission efficiently and effectively by introducing uncertainty and requiring re-training of all intelligence professionals on new policies and procedures implementing ever-changing authorities. Moreover, over the past year, in the interest of providing an extensive legislative record and allowing public discussion on this issue, the Intelligence Community has discussed in open settings extraordinary information dealing with intelligence operations. To repeat this process in several years will unnecessarily highlight

our intelligence sources and methods to our adversaries. There is now a lengthy factual record on the need for this legislation, and it is time to provide the Intelligence Community the permanent stability it needs.

Fails to Provide Procedures for Implementing Existing Statutory Defenses. The Judiciary Committee substitute fails to include the important provisions in the SSCI bill that would establish procedures for implementing existing statutory defenses and that would preempt state investigations of assistance allegedly provided by an electronic communication service provider to an element of the Intelligence Community. These provisions are important to ensure that electronic communication service providers can take full advantage of existing liability protection and to protect highly classified information.

Fails to Address Transition Procedures. Unlike the SSCI bill, the Judiciary Committee bill contains no procedures designed to ensure a smooth transition from the PAA to new legislation, and for a potential transition resulting from an expiration of the new legislation. This omission could result in uncertainty regarding the continuing validity of authorizations and directives under the Protect America Act that are in effect on the date of enactment of this legislation.

Fails to Include a Severability Provision. The Judiciary Committee substitute, unlike the SSCI bill, lacks a severability provision. Such a provision should be included in the bill.

* * *

The Administration is prepared to continue to work with Congress towards the passage of a permanent FISA modernization bill that would strengthen the Nation's intelligence capabilities while protecting the constitutional rights of Americans, so that the President can sign such a bill into law. The Senate Intelligence Committee bill provides a solid foundation to meet the needs of our Intelligence Community, but the Senate Judiciary Committee bill represents a major step backwards from the PAA and would compromise our Intelligence Community's ability to protect the Nation. The Administration calls on Congress to forge ahead and pass legislation that will protect our national security, not weaken it in critical ways.

* * * * *