FISA Legislation Necessary To Keep Our Nation Safe

Congress Must Act To Make Collection Authority
Under The Protect America Act Permanent And
Provide Meaningful Liability Protection To Telecommunications Companies

"The legislation Congress approved early this year to make sure our intelligence professionals can continue to effectively monitor terrorist communications is set to expire in February. Allowing this law to lapse would open gaps in our intelligence and increase the danger to our country. Our intelligence professionals need these tools to keep our people safe, and they need Congress to ensure that these tools are not taken away."

-President George W. Bush 12/4/07

In August, Congress passed the Protect America Act with bipartisan support to close a critical intelligence gap that was making our Nation less safe. The Protect America Act (PAA) modernized the Foreign Intelligence Surveillance Act of 1978 (FISA) to provide our Intelligence Community essential tools to acquire important information about terrorists who want to harm America. It restored FISA to its original focus of protecting the rights of persons in the United States, while not acting as an unnecessary obstacle to gathering foreign intelligence on targets located in foreign countries.

- **The essential tools provided by the Protect America Act will expire in less than two months, and Congress must act to keep our Nation safe by making these tools permanent.** The Senate is considering FISA modernization legislation this week. Already, the Senate Select Committee on Intelligence (SSCI) has approved a bipartisan bill that, while not perfect, is a significant step in the right direction.

- **The Administration looks forward to continuing its work with Congress on a bill that keeps our Nation safe by making the critical authority to collect intelligence under the PAA permanent and by providing meaningful liability protection to companies facing multi-billion dollar lawsuits only because they are believed to have assisted in the efforts to defend our Nation following the 9/11 attacks.**

<u>The PAA And The Bipartisan SSCI Bill Maintain Strong Oversight Provisions To Protect The Rights Of Americans In The United States</u>

The PAA and the bipartisan SSCI bill provide for FISA Court review of the procedures for determining that the acquisition of foreign intelligence information under the legislation concerns persons reasonably believed to be located outside the United States. This approach provides a useful role for the FISA Court.

Strong oversight mechanisms for all intelligence collection authorized by the PAA already exist within the executive branch. Under the PAA, the Justice Department and the Office of the Director of National Intelligence must perform regular reviews of intelligence collection. In addition,

the internal compliance office of any agency that collects intelligence under the PAA must perform regular reviews to ensure the agency is complying with the PAA.

Requiring Intelligence Officials To Apply For Court Orders Before Collecting Foreign Intelligence From Overseas Targets Would Make Our Nation Less Safe

The PAA and the bipartisan SSCI bill restore FISA to its original focus of protecting the rights of Americans within the United States while making clear that – as was the intent when Congress enacted FISA in 1978 – advance court approval is not required to target persons located overseas. When FISA was enacted 30 years ago, the law did not generally require a court order to obtain foreign intelligence information from a target located outside the United States. Unforeseen changes in technology, however, meant that prior to passage of the PAA, the government often needed to obtain a court order before vital intelligence collection could begin against a terrorist or other foreign intelligence target located in a foreign country.

A mandatory prior court approval process would create delays that could prevent the swift gathering of intelligence necessary to identify and provide warning of threats to our country.

Any Legislation Should Grant Meaningful Liability Protection To Companies Believed To Have Assisted In Efforts To Defend Our Nation Following The 9/11 Attacks

As recognized by the bipartisan SSCI bill, those companies alleged to have assisted the government in the aftermath of September 11th should not face massive and costly litigation for helping protect our country. Such litigation risks the disclosure of highly classified information and could lead to reduced intelligence collection capabilities in the future by discouraging companies from cooperating with the government.

Senate Select Committee on Intelligence Chairman John D. Rockefeller (D-WV) has agreed with this point, writing "we must preserve the cooperation of private industry for the next president, and for every one who follows." "The fact is, private industry must remain an essential partner in law enforcement and national security. We face an enemy that uses every tool and technology of 21st-century life, and we must do the same. If American business – airlines, banks, utilities and many others – were to decide that it would be too risky to comply with legally certified requests, or to insist on verifying every request in court, our intelligence collection could come to a screeching halt. The impact would be devastating to the intelligence community, the Justice Department and military officials who are hunting down our enemies." (John D. Rockefeller IV, Op-Ed, "Partners In The War On Terror," *The Washington Post*, 10/31/07)

Former CIA Director R. James Woolsey also stressed the importance of liability protection, saying companies "were helping solely out of a sense of patriotism and an understanding that some steps that the nation needs to take in a dangerous world cannot be taken in public." "We live in a world of terrorism, the possible proliferation of nuclear weapons and a host of other risks to our security. Intelligence, and the cooperation of the private sector in obtaining and protecting it, will be among our most important tools to avoid catastrophes such as Sept. 11 or worse." (R. James Woolsey, Op-Ed,

"Private Help For The Public Good Shouldn't Lead To Litigation," *San Jose* [CA] *Mercury News*, 11/16/07)

9/11 Commission Co-Chairman Lee Hamilton similarly agreed that "the increasing complexity of communications technology has made the voluntary cooperation of these companies vital." "The help and cooperation of all our citizens are vital in combating the threats we face today. Companies in various sectors of the economy are going to have information that could save the lives of thousands of Americans. When they respond in an emergency, at the call of our highest elected officials and on assurances that what they are doing is legal, they must be treated fairly. To do otherwise would put our security at risk. This is particularly true of communications companies. They are critical to our intelligence and 'early warning' against terrorist attacks." (Lee Hamilton, Op-Ed, "Immunity For Wiretap Assistance Is Right Call," *The Baltimore Sun*, 11/4/07)

While It Is An Important Step In The Right Direction, The SSCI Bill Does Contain Some Troublesome Provisions

The so-called "Wyden Amendment" to the SSCI bill would require for the first time that a court order be obtained to surveil U.S. persons abroad. In addition to having serious technical problems, this provision would impose burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes.

The SSCI bill contains a six-year sunset, which the Administration opposes. While this limitation is preferable to the even shorter sunset in the House legislation, the vital authorities to surveil overseas targets should be put on a permanent footing. Any sunset period introduces a significant level of uncertainty as to the rules employed by our intelligence professionals and followed by private partners.

The SSCI bill contains a reporting requirement that poses serious operational difficulties for the Intelligence Community. The SSCI bill contains a requirement that intelligence analysts count "the number of persons located in the United States whose communications were reviewed." This provision might well be impossible to implement. In addition, it does not reflect the way in which intelligence analysis is conducted – for instance, once analysts determine that a communication is not relevant, they move on to the next piece of information; they do not analyze the irrelevant communication to determine the location of the persons who were parties to the communication. To require analysts to do so would not only waste resources but also pose a needless intrusion on privacy.

The Basics Of FISA: Why Legislation Is Necessary To Bring The Law Up To Date

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 to regulate the Government's efforts to conduct certain foreign intelligence surveillance activities directed at persons in the United States. Congress recognized that the Government must be able to effectively collect foreign intelligence about those who wish to harm our country. To allow this collection to proceed while protecting the rights of Americans in the

United States, Congress established a process for judicial approval that generally applied when the government targeted persons located inside the United States for foreign intelligence surveillance – but that generally did not apply to activities directed at persons overseas.

Revolutionary advances in telecommunications technology since 1978 upset the careful balance established by Congress to distinguish between surveillance governed by FISA and surveillance directed at targets outside the U.S. The mechanism Congress used to identify which activities fell within FISA's scope – and to strike the balance between surveillance directed at persons overseas and persons in the United States – was a careful and complex definition of the term "electronic surveillance." This definition was framed in terms of the specific communications technologies used in 1978.

As a result, prior to the Protect America Act, the Government often needed to obtain a court order before vital intelligence collection could begin against a terrorist or other foreign intelligence target located in a foreign country. These targets often were communicating with other foreign persons overseas, but FISA's court order requirement still applied. It made no sense to require the Government to obtain a court order to collect foreign intelligence on targets located in foreign countries – nor was such a requirement generally intended when Congress passed FISA nearly 30 years ago.

This requirement resulted in a critical intelligence gap that was making our Nation less safe. Requiring the Government to go to court before the collection of foreign intelligence could begin resulted, as the Director of National Intelligence put it, in our intelligence professionals "missing a significant amount of foreign intelligence that we should be collecting to protect our country."

By changing FISA's definition of electronic surveillance to clarify that the statute does not apply to surveillance directed at overseas targets, the Protect America Act has enabled the Intelligence Community to close this critical intelligence gap. The Protect America Act makes clear – consistent with the intent of the Congress that enacted FISA in 1978 – that our Intelligence Community should not have to get bogged down in a court approval process to gather foreign intelligence on targets located in foreign countries. It does not change the strong protections FISA provides to people in the United States. FISA's definition of electronic surveillance remains unchanged for surveillance directed at people in the United States and continues to require court approval as it did before.

The vital authorities to surveil overseas targets under the PAA will expire in less than two months, and Congress must act to keep our Nation safe by making these provisions permanent.