U.S. Department of Justice

National Security Division

Assistant Attorney General *Washington, D.C. 20530*

SEP 14 2007

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Reyes:

I write this letter in response to questions posed by you and other Members of the House Permanent Select Committee on Intelligence at its hearing on September 6, 2007, concerning the scope of the Protect America Act of 2007. You requested that certain answers given at that hearing be provided in writing and -- to the extent possible consistent with the national security -- in an unclassified format.

I appreciate your invitation to provide our thoughts on these matters as you evaluate the Protect America Act and consider our request to make the legislation permanent. I believe that this dialogue is a healthy process, and that it will help provide assurance to the American public and the Congress that the Act is a measured and sound approach to an important intelligence challenge.

The passage of the Protect America Act was a significant step forward for our national security. As this Committee is aware, sweeping changes in telecommunications technologies since the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978 expanded the scope of the statute substantially. As a result of these technological changes -- and not of any deliberate choice by the Congress -- the Executive Branch frequently was required to seek court approval, based upon a showing of probable cause, to conduct surveillance targeting terrorists and other foreign intelligence targets located overseas. This created a significant gap in our intelligence capabilities with no corresponding benefit to the civil liberties of persons in the United States.

By changing FISA's definition of electronic surveillance to clarify that the statute does not apply to surveillance directed at overseas targets, the Congress has enabled the Intelligence Community to close critical intelligence gaps, and the nation is already safer because of it. We urge the Congress to make the Protect America Act permanent, and also to enact the other important FISA reforms contained in the comprehensive FISA Modernization proposal we submitted to Congress earlier this year. It is especially imperative that Congress provide liability protection to companies that are alleged to have

assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

At the hearing last week, you and other Members of the Committee asked several specific questions concerning whether the Protect America Act hypothetically could authorize the Government to engage in certain intelligence activities that extend beyond those you contemplated when Congress passed the legislation. We appreciate the opportunity to provide you with answers, as these and other such questions have also been asked by other members of Congress and by members of the public.

While we understand the civil liberties concerns underlying these various questions, there are several reasons why this legislation does not give rise to these concerns. First, most of the hypotheticals we have heard are inconsistent with the plain language of the Protect America Act and the rest of the FISA statute. Second, we commit that we will not use the statute to undertake intelligence activities that extend beyond the clear purpose of the statute. And third, we will apply the statute in the full view of congressional oversight, as we intend to provide Congress with consistent and comprehensive insight into our implementation and use of this authority. As we have publicly committed, we will inform the full membership of the Intelligence and Judiciary Committees concerning the implementation of this new authority and the results of the reviews that this Division and the Office of the Director of National Intelligence are conducting to assess and ensure compliance by the implementing agencies; we will provide you copies of the written reports of those compliance reviews; and we will make ourselves available to brief you and your staffs about compliance and implementation on a monthly basis throughout this renewal period. In fact, representatives of the Executive Branch already have provided several detailed briefings to Committee Members and staff on the implementation of the Protect America Act since its passage. In addition, we have provided the committees with copies of documents related to our implementation of this authority, including the relevant certifications and procedures required by the statute (with redactions as necessary to protect critical intelligence sources and methods). With such comprehensive reporting to Congress, you and your colleagues will be able to see and assure yourselves that we are implementing this new authority appropriately, responsibly, and only in furtherance of the purposes underlying the statute.

****

I would like to address several of the hypothetical situations you and your colleagues raised at the hearing last week, and explain why we believe they will not arise under our implementation of the Protect America Act.

First, questions arose at the hearing concerning the Protect America Act's application to domestic communications, and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located

outside of the United States," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words, the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2) -- a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, several Members of the Committee asked whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the Government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications -- further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for such purposes.

Third, a question was asked about whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, we do not think that this provision authorizes the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, and finally, it was suggested that this letter be used as an opportunity for the Executive Branch to allay concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA -- because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1) -- and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance directed at targets overseas. Because it would remain a violation of FISA, the Government cannot -- and will not -- use this authority to engage in "reverse targeting."

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in "reverse targeting." If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target's calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target's communications.

****

Thank you again for the opportunity to appear at your hearing last week, and to provide these responses to your thoughtful questions. I hope you find this input helpful. Because we believe that these responses will likely be of interest to the Senate Select Committee on Intelligence and the Judiciary Committees, I have sent copies of this letter to the Chairman and Ranking Member of each of those committees.

Please do not hesitate to call on me or my colleagues if we can be of further assistance as you consider FISA modernization and the renewal of the Protect America Act.

Sincerely,

Kenneth L. Wainstein
Assistant Attorney General

cc: Sen. Rockefeller
Sen. Bond
Sen. Leahy
Sen. Specter
Rep. Hoekstra
Rep. Conyers
Rep. Smith