STATEMENT FOR THE RECORD OF

LT GEN KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

JULY 26, 2006

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee.

I am pleased to be here today to provide testimony in support of the National Security Surveillance Act of 2006 (S. 2453), which would amend the Foreign Intelligence Surveillance Act of 1978. The changes proposed in the bill are, I believe, intended to recapture the original Congressional intent of the statute – ensuring the protection of the rights of people in the United States as the Government engages in electronic surveillance. At the same time, the proposed bill would remove from the statute's coverage surveillance directed at individuals who are not due protection under the Fourth Amendment, such as foreign persons located overseas.

While some of the specifics that support my testimony and support passage of this bill cannot be discussed in open session, and while I would be happy to elaborate on the technological changes that have taken place since 1978 in an appropriate setting, the essential point can be made very clearly and publicly: communications technology has evolved in the 28 years between 1978 and today in ways that have had unforeseen consequences under the statute. While the FISA as originally drafted incorporated the unique features of 1978 technology to achieve agreed-upon goals, the stunning technological changes in the communications environment that we have witnessed since that time have brought within the scope of the statute communications that we believe the 1978 Congress did not intend to be covered.

Today, the U.S. Government is often required by the terms of the statute to make a constitutionally based showing of probable cause in order to target for surveillance the communications of a foreign person overseas. Frequently, though by no means always, that person's communications are with another foreign person overseas. Obtaining a court order, based on the constitutionally required showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security. In that respect, we frequently sacrifice to detailed and rigorous process one of our greatest advantages in our effort to collect foreign intelligence – the ability to access a vast proportion of the world's communications infrastructure located in our own nation.

The FISA sought – in simple terms – to permit the surveillance of foreign intelligence targets, while providing appropriate protection through Court supervision to U.S. citizens and to other persons in the United States. As the legislative history of the 1978 statute stated: "[t]he history and law relating to electronic surveillance for 'national security' purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary for the security of the nation and the requirements of the Fourth Amendment."[1] While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, the judgment of Congress at that time was that Court supervision was important -- if not absolutely essential -- when significant Fourth Amendment interests were implicated.

Yet the Fourth Amendment is clearly not always at issue when NSA or another intelligence agency acts, and the FISA surely never sought to encompass all activities of the NSA within its coverage. Rather, the definitions of the term "electronic surveillance" contained in the statute have always affected just a portion of NSA's signals intelligence mission. Indeed, by far the bulk of NSA's surveillance activities take place overseas, and these activities are directed entirely at foreign countries and foreign persons within those countries. All concerned agree, and to my knowledge have always agreed, that the FISA does not and should not apply to such activities. When NSA undertakes surveillance that does not meet any of the definitions of electronic surveillance contained in the FISA, it does so

---

[1] H. Rep. 95-1283 at p. 15, 95th Congress, 2d Session June 8, 1978.

without any resort to the court and without reliance on a showing of probable cause.

In addition, even as it engages in its overseas mission, in the course of targeting the communications of foreign persons overseas, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities, and to my knowledge no serious argument exists that it should. Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities, seeking through these procedures to minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades at ensuring the constitutional reasonableness of NSA's surveillance activities, and at eliminating from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence. Accomplishing this has not required a court order.

Because of the way the definitions of "electronic surveillance" contained in the current statute are constructed, the answers to several questions are relevant to the determination of whether a FISA order is required in order for NSA to engage in electronic surveillance. These questions concern the nationality of the target, the location of the target, the means by which the target is communicating, and the location from which the surveillance will be carried out. We believe that the truly significant question on this list is the one that gets to the heart of the applicability of the constitution – the location of the target of surveillance. The other questions reflect a common sense approach to 1978 technology that worked well in 1978, but that today appears to have unintended effects.

In many cases, the decision whether the Government must obtain an order from the FISA Court, and in doing so must make a showing that relies on the constitutional notion of probable cause, depends in part on such issues as the communications technology employed and the location in which the collection efforts take place. We believe such issues to be ancillary, if not irrelevant, to the more fundamental issue. Thus, in some cases, whether NSA seeks to acquire a communication from inside the United States, or seeks to acquire the very same communication outside the United States, becomes a question clothed in undue significance. So, too, the technology employed by the provider of the communications service can in some cases

be dispositive of whether the Government must obtain a FISA order or not. We think this is far from what was intended by the statute's supporters in 1978, and requires change.

Senate Bill S. 2453 would effect the required change, making relevant only those questions that independently carry-significance - particularly in the telecommunications environment of 2006. Principally, the issue on which the need for a Court Order should turn – but does not turn under the current FISA -- is whether or not the person whose communications are targeted is generally protected by the guarantees of the constitution. That question, in turn, is largely determined by the location of the target. People inside the United States who are the targets of electronic surveillance, irrespective of where the surveillance is conducted or what means are used to transmit a communication, would receive under this Bill the protection afforded by Court approval. At the same time, people outside the United States who are not U.S. persons, again irrespective of where the surveillance is effected or the technology employed, would not receive such protection. Targeting of U.S. persons outside the United States would be treated exactly as it is today, only with specific approval of the Attorney General based on appropriate findings. In short, we believe the bill currently under consideration contains language appropriate to restore to the statute appropriate protection of those who are located in the United States.

Moreover, the current FISA – at least in some places – already recognizes the principles the bill seeks to inject throughout the statute. As I have noted already, we think the most significant factor in determining whether or not a Court Order is required ought to be the location of the target of the surveillance, and that other factors such as where the surveillance takes place and the mode of communication surveilled should not play a role in this determination. Significantly, this was quite precisely recognized in the legislative history of the current statute with respect to the first of the definitions of electronic surveillance – the intentional targeting of the communications of a U.S. person in the United States. The legislative history makes clear with respect to that definition that when the communications of U.S. persons located in the United States are targeted, the surveillance is within the scope of FISA irrespective of whether the communications are domestic or international and likewise irrespective of where the surveillance is being carried out.[2] The same legislative history

[2] Id. at 50.

regarding that first definition of electronic surveillance makes equally clear, however, that the statute does not regulate the acquisition of communications of U.S. persons in the United States when those persons are not the actual targets of the surveillance.[3]

We think these principles, clearly and artfully captured in parts of the legislation and in the legislative history, should extend to all surveillance under the FISA. The need for a court order should not depend on whether NSA's employees conducting the surveillance are inside the United States or outside the United States, nor should it depend on whether the communications meet the technical definition of "wire communications" or not. These factors, never directly relevant in principle but once relevant in the context of yesterday's telecommunications infrastructure, are today utterly irrelevant to the central question at issue – who are the people requiring protections. Whether surveillance should require Court supervision ought to depend on whether the target of such surveillance is located within the United States.

In addition to changes to the definition of electronic surveillance, other changes in the bill are important as well. First, and most crucially, the Government must retain a means to compel communications providers to provide information to the Government even in the absence of a Court Order. The Bill would authorize the Attorney General to require such cooperation, and would also insulate from liability those companies that assist the IC in preventing future attacks on the United States.

Finally, other changes are not as crucial to the continued success of the intelligence community in countering threats, but will make a better bill. For instance, the bill recognizes the inadequacy of the manner in which FISA defines the phrase "agent of a foreign power," and adds to the category visitors to the United States who may not be working for a particular government and may not be terrorists, saboteurs or spies, but who nonetheless have and may transmit or receive significant foreign intelligence information.

---

[3] Id.

Let me reiterate in closing that we believe the statute should be updated to account for changes that have taken place in technology since its initial passage. Furthermore, we think the appropriate way to change the statute is to focus on significant factors, while setting aside ancillary issues such as the technical means employed or the location from which the surveillance was conducted.