STATEMENT FOR THE RECORD OF

ROBERT L. DEITZ
GENERAL COUNSEL, NATIONAL SECURITY AGENCY

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 6, 2006

Good morning Mr. Chairman, Ranking Member Scott, and Members of the Committee.

I am pleased to be here today to provide testimony in support of legislative efforts to amend the Foreign Intelligence Surveillance Act of 1978. Changes are needed, I believe, in order to recapture the original Congressional intent of the statute -- regulating the electronic surveillance of persons within the United States -- as the Government engages in electronic surveillance. At the same time, surveillance directed at individuals who are not due protection under the Fourth Amendment should be removed from the statute's coverage.

Some of the specifics that support my testimony 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 FISA. These stunning technological changes in the communications environment have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered and that were excluded from the Act's scope.

Despite this change, NSA's mission remains the same. NSA intercepts communications to protect the lives, the liberties, and the well-being of the citizens of the United States from those who would do us harm. Today, NSA is often required by the terms of FISA to make a showing of probable cause, a notion derived from the Fourth Amendment, 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. In such cases, the current statutory requirement to obtain a court order, based on a 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.

The FISA seeks – we believe - 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 states: "[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]

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

While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that it was only when significant Fourth Amendment interests were implicated that court supervision was important .

Yet the Fourth Amendment is clearly not always at issue when NSA or another intelligence agency acts, and the FISA on its face 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 lawfully under Executive Order 12333 without any resort to the FISA court.

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 to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate 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 definition of "electronic surveillance" contained in the current statute is constructed, NSA must answer four questions in order to determine whether a FISA order is required for it 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 then, but that today has unintended effects. They are ancillary, if not irrelevant, to the more fundamental issue.

Thus, in some cases, the location from which NSA seeks to acquire a communication 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.

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, regardless of where the surveillance is conducted or what means are used to transmit a communication, should be the only ones who receive the protection afforded by court approval. At the same time, people outside the United States who are not U.S. persons, again regardless of where the surveillance is effected or the technology employed, should not receive such protection. The FISA should be returned to what we believe was its original purpose of regulating foreign surveillance targeting persons in the United States, not the surveillance of non-U.S. persons overseas who are not entitled to constitutional rights.

Moreover, the current FISA - at least in some places - already recognizes this principle. 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 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. We believe 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 regardless of whether the communications are domestic or international and regardless of where the surveillance is being carried out.[2] The same legislative history 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 were never directly relevant in principle, but in the context of yesterday's telecommunications infrastructure were used as a proxy for relevant considerations. Today they are utterly irrelevant to the central question at issue: who are the people deserving protection. 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 changing the definition of electronic surveillance, other changes are needed as well. For example, it is vitally important that the Government retain a means to

[2] Id. at 50.
[3] Id.

compel communications providers to provide information to the Government, even in the absence of a court order. It is also critical that companies assisting the Intelligence Community in preventing future attacks on the United States be insulated from liability for doing so.

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 constitutionally significant factors that will ensure that the rights of U.S. citizens are protected, while setting aside ancillary issues such as the technical means employed or the location from which the surveillance was conducted.