Hearing of the

United States Senate

Select Committee on Intelligence

Tuesday, May1, 2007

Testimony of Suzanne E. Spaulding

I want to thank the Senate Select Committee on Intelligence for this opportunity to submit testimony in the context of the May 1, 2007, hearing on the Foreign Intelligence Surveillance Act (FISA).

I'd like to begin by emphasizing that I have spent over twenty years working on efforts to combat terrorism, including serving as General Counsel and Deputy Staff Director of this committee in the mid-90s. Over those two decades, in my work at the Central Intelligence Agency, at both the House and Senate intelligence oversight committees, and as Executive Director of two different commissions on terrorism and weapons of mass destruction, I developed a strong sense of the seriousness of the national security challenges that we face and deep respect for the men and women in our national security agencies who work so hard to keep our nation safe.

We owe it to those professionals to ensure that they have the tools they need to do their job; tools that reflect the ways in which advances in technology have changed the nature of the threat and our capacity to meet it. Equally important, they deserve to have careful and clear guidance on just what it is that we want them to do on our behalf -- and how we want them to do it. Clear rules and careful oversight provide essential protections for those on the front lines of our national security efforts.

This is particularly critical with regard to the collection and exploitation of intelligence related to threats inside the United States, which I will refer to as domestic intelligence.[1] The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The Federal Bureau of Investigation's priorities turned 180 degrees, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state and local law enforcement are among the many entities gathering intelligence inside the US. The collection of information on the movement, communications, and activity of any international terrorists that may be targeting and operating in the US presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion.

Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

Rather than continuing this pattern, I urge Congress not to consider the kind of dramatic and far-reaching overhaul of FISA that has been proposed by the

[1] Included in this concept of domestic intelligence is any intelligence that involves a domestic component, such as the interception of communications between someone in the US and someone outside the country. This does not pre-suppose how that intelligence ultimately should be treated but acknowledges that it raises potentially different issues than intelligence involving purely foreign components.

Administration without first undertaking a comprehensive review of domestic intelligence.

A Joint Inquiry or Task Force could be established by the Senate leadership, with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, and Homeland Security and Government Affairs), to carefully examine the nature of the threat inside the US and the most effective strategies for countering it. Then Congress, and the American public, can consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, how does the authority proposed for a new FISA section 102A relate to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, the pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes? And how do these techniques relate to more intrusive investigative and intelligence tools?

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance to eavesdrop on Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. It's not the "all or nothing" proposition often portrayed in some of the debates.

The recent report by the Inspector General on the misuse of national security letter authority found, similarly, that while Attorney General guidelines on National Security Investigations also cite the requirement to use the least intrusive techniques feasible, there is not sufficient guidance on how to apply that in the national security letter context or in conjunction with other available collection techniques.

Many of these authorities, moreover, have been amended since 9/11 in ways that seem to permit the gathering of vast amounts of information that could then be used for purposes of data mining. Some kinds of data mining could provide essential national security capabilities that the government should be actively researching and developing. Unfortunately, equally essential public discussion and debate about appropriate policies to govern data mining implementation were cut short by the public reaction to early proposals such as Total Information Awareness. Thus, the legal authority to collect the information continued to expand without adequate consideration of safeguards to ensure appropriate use of that information. Some of the proposed changes to FISA would further exacerbate this trend. This needs to be considered more comprehensively.

Additionally, while there has been much public debate about the role of the FBI, there has been very little discussion about the domestic intelligence activities of other agencies such as CIA and the Defense Department. For example, executive branch lawyers assert that the Global War on Terrorism (GWOT) is a war in the full legal sense and the battlefield is wherever suspected terrorists are or might be in the future. Intelligence collection is a key aspect of preparing the battlefield and an important aspect of DOD's homeland defense mission. Moreover, section 1681v of the Fair Credit Reporting Act allows any agency engaged in counter-terrorism analysis, including presumably DOD, to demand consumer reports on US citizens and others. Congress needs to understand exactly what DOD is doing inside the United States

and promote a robust and informed discussion about what it is we want them to be doing. Under what legal authorities is it operating? Should DOD meet its own intelligence requirements inside the United States or should the FBI or some other entity be responsible for gathering information for all those who need it, including DOD?

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the US, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.

This applies to the proposed changes to FISA, as well. Congress must be certain that it has been fully informed about the details of the Terrorist Surveillance Program and any other surveillance programs or activities initiated after 9/11, not just in their current form but in the very earliest stages. Understanding how the law operates in times of crisis and stress is key to understanding how it might need to be strengthened or adjusted.

A fundamental concern with the FISA overhaul proposed in this legislation is that the government has not adequately explained to the American public, and perhaps even to Congress, precisely why these changes are necessary and justified. It is reasonable to assume that some changes to FISA—in addition to all of the changes already made since 9/11-- might be appropriate to address changes in technology. For example, communications between non-USPs outside the United States are not subject to FISA. They should not suddenly fall within FISA's scope simply because they happen to transit the US.

However, many of the changes to FISA proposed in this legislation are troubling. I will highlight a few of the most significant in my testimony today.

Among the changes of greatest concern are those made to the definitions of terms used throughout the FISA statute. Changing the meaning of those terms has potentially far-reaching consequences that are not always readily apparent without a detailed analysis of each place in the statute where the term is used. In addition, FISA definitions inform the use of these terms in numerous other contexts, such as intelligence directives and policies.

Changes that raise particularly significant concerns include:

Electronic surveillance: The safeguards of FISA with regard to electronic communications apply almost exclusively to "electronic surveillance." The bill appears to exclude from that definition, and thereby allow warrantless interception of, calls or emails of persons, including US citizens, inside the US who are communicating with persons, again including US citizens, outside the US, so long as the government is not directing the intercepts at a *known* US person (USP) inside the US. Note that this exemption from FISA would not be limited to communications in which a suspected terrorist or other agent of a foreign power was at one end of the call.

Surveillance devices: The changes would also seem to allow, without a warrant, broader use of a wide range of surveillance devices against US citizens and others. Part of the current definition of "electronic surveillance" includes installation of *any* surveillance device (e.g., camera, infrared sensor, etc.) inside the US under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Under the proposed amendments, such surveillance devices would only be covered by FISA if they are

intentionally directed at a particular, known USP. As a result, conducting such technical surveillance, even under circumstances where there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes--such as in a private meeting facility or place of worship--would now seem to be defined-out of FISA, so long as the government is not targeting a particular, known US person.

Agent of a Foreign Power: The bill would broaden this definition to include any non-US person who possesses, or is expected to receive, "foreign intelligence information," a term that was earlier amended to include any information that relates to "the ability of the United States to protect against actual or potential attack." The person possessing the information does not need to have any connection with terrorist activities, let alone a terrorist group or other foreign power. The bill does not require that the person provide this information to anyone or even ever contemplate giving it to anyone; merely possessing the information makes you an agent of a foreign power. Vast categories of privately held information that have nothing directly to do with terrorist attacks, including information about co-workers or classmates, or building blueprints, might be determined by the government to be related to the ability to protect against a potential attack. Any non-USP the government decided possessed such information, even if they worked for a US company or US newspaper, would be an agent of a foreign power and thus potentially subject to having the government not only seize the information but intercept their communications or secretly search their premises. Since even non-USPs are guaranteed the protections of the Fourth Amendment, this change could raise serious concerns about the continued constitutionality of FISA.

Weapons of Mass Destruction. The definition of an agent of a foreign power is further broadened to include persons engaged in the development of weapons of mass destruction (WMD). It is not clear why existing laws, including FISA provisions related to preparations for sabotage, etc., are not adequate. Moreover, the definition of WMD is broad and vague. It includes "any destructive device"-- not just chemical, biological, nuclear, or radiological devices-- intended or *capable of* killing or seriously injuring "*a significant number of people*." Another part of the definition includes any weapons intended to cause death or injury through release of toxic chemicals, which could cover the assassination of a single individual with a toxic umbrella tip. And there is no requirement for any foreign connection, since even the definition of a foreign power would be amended to include any "group engaged in the proliferation of weapons of mass destruction." Again, this moves still further away from the original justification, articulated by the courts and Congress, for the unique, secret intelligence authority provided in FISA.

Minimization Procedures: The proposed legislation would significantly alter the safeguards currently applicable to surveillance authorized by the Attorney General, while at the same time expanding that unilateral authority far beyond its initial scope of simply foreign power to foreign power communications. Under current law, if surveillance is conducted pursuant to AG authorization rather than a warrant from a FISA judge, no contents of any communication to which a USP is a party can be disclosed, disseminated, or used for any purpose or retained for more than 72 hours without getting a court order, unless the AG determines that the information indicates a threat of death or serious bodily harm. Concern about ensuring that electronic surveillance authorized unilaterally by the AG could not be used to gather information about USPs was so strong when FISA was enacted that even the mere existence of

such a communication (included in the current definition of "contents") was included in this restriction. This entire section is deleted in the proposed bill.

Instead, under the proposed legislation, broad unilateral AG authority would be statutorily subject only the weaker procedures that currently apply in instances where a FISA judge has reviewed an application to ensure that the target is a foreign power or an agent of a foreign power. These simply require procedures reasonably designed to "minimize" the acquisition and retention of USP information "consistent with the need to obtain, produce, and disseminate foreign intelligence information." The AG is also freed from the requirement to certify that "there is no substantial likelihood" that the surveillance will acquire a communication to which a USP is a party. This loosening of restrictions with regard to US person conversations is disturbingly consistent with, and exacerbated by, proposed changes in Section 102 that expand the AG's power to authorize warrantless surveillance of conversations involving USPs, so long as the target is a foreign power.

Contents: The proposal would eliminate from the definition of "contents" information about the identities of the parties and the existence of the communication. Instead, it would be limited it to the "substance, purport, or meaning" of the communication. The argument for this change is that it conforms the FISA definition to the one contained in the statute pertaining to communications intercepts in criminal investigations and will conform the FISA pen register/trap-and-trace authorities with their counterparts in the criminal context. Congress needs to ensure that it fully understands the potential impact of this change.

First, this change does not just affect pen register and trap-and-trace authority. The term "contents" informs other key definitions and authorities in FISA. Under the new definition of electronic surveillance, for example, even the interception of

purely domestic calls or emails would not be covered under FISA so long as the government was not intentionally acquiring the "contents" of those calls or targeting a particular, known USP. This would seem to allow the interception of purely domestic calls if the government only "acquired" information such as the gender of the parties, the tone of voice, the language spoken, etc.

As noted earlier, FISA's current broader definition of "contents" reflects the particular sensitivity of secretly intercepting calls of US citizens in a context where the normal safeguards and transparency built into our criminal system do not apply. Moreover, it is not clear what impact changing this definition might have in other contexts, such as NSA's ability to search its databases for USP names. At a minimum, Congress should consider only applying this change to the pen register and trap-and-trace provisions rather than the entire statute.

There are many more potential problems with the changes in this legislation. These include, in addition to the dramatic expansion of unilateral AG authority, expanding the role of FISA judges and the Foreign Intelligence Surveillance Court of Review in a way that reduces the check currently provided by the knowledge that their decisions might be reviewed by a regular Article III judge, and the vast expansion of certifying authority beyond the ranks of politically-accountable Presidential appointees to anyone in the executive branch.

The proposed extremely broad blanket immunity for the telecommunication companies and others also deserves particularly careful examination. It's not clear why this is needed. In an area such as this, where the normal safeguards of transparency are lacking, requiring communication providers to at least get a certification that the request to hand over customer information or allow

communication intercepts is legal serves as an important potential deterrent to abusive behavior by the government. Congress needs to fully understand what past activities would be immunized before adopting such a wide-ranging provision.

FISA is the primary statute governing domestic intelligence collection. Rather than attempt to fix this proposal and guess at what might really be needed to meet today's challenges, Congress should take the time to ensure they understand the full context in which these changes are being sought. This includes the problems that have prompted them, particularly as these relate to current and past intelligence activities and the changing nature of the threat, as well as how these new authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.